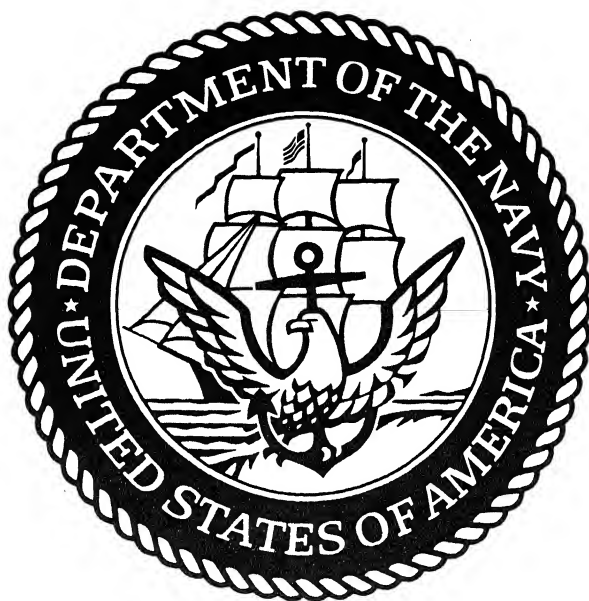




DEPARTMENT OF THE NAVY



PHYSICAL SECURITY AND LOSS PREVENTION



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

IN REPLY

OPNAVINST 5530
OP-09N/NIS-01
16 September 1

OPNAV INSTRUCTION 5530.14A

From: Chief of Naval Operations

Subj: Physical Security and Loss Prevention

Encl: (1) Physical Security and Loss Prevention Manual

1. Purpose. To establish policy, provide guidance and set forth uniform standards for physical security measures to safeguard Navy personnel, property and material at Navy shore activities. References cited in this manual are contained in Appendix I.

2. Cancellation. OPNAV Instruction 5530.14.

3. Scope. Enclosure (1) addresses physical security and loss prevention responsibilities, physical security measures and minimum criteria for physical security.

4. Discussion. To be effective, a physical security program must receive command attention and direction from all echelons within the chain of command, and physical security functions must be carried out by properly trained and equipped personnel. Emphasis is placed on the commanding officer's responsibility to ensure that the command security posture is accurately assessed and security resources are appropriate to execute these programs.

5. Responsibilities. Security is the direct, immediate and moral responsibility of all persons in the naval service and civilians employed by the Department of the Navy.

a. Commanding officers are responsible for physical security and loss prevention within their commands.

b. The security officer is the designated representative of the commanding officer responsible for planning, implementing, enforcing and supervising the physical security and loss prevention programs of the command.

c. Echelon two commanders are responsible for overseeing implementation of this instruction to include checking for compliance throughout subordinate activities.

OPNAVINST 5530.14A

16 SEP 1985

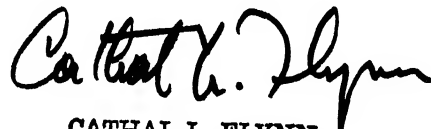
6. Applicability. This instruction is applicable to all shore activities and to all naval military and civilian personnel employed/located thereon.

7. Action

a. The Naval Inspector General will conduct oversight checks of naval activities to determine compliance with requirements contained in this instruction.

b. Commanding officers at all echelons will evaluate physical security and loss prevention programs of their activities, and ensure compliance with this instruction.

8. Forms. OPNAV 5527/1 (Rev. 12/82), Incident/Complaint Report, S/N 0107-LF-055-2705, is available through normal supply channels in accordance with NAVSUP P-2002. Option Form 55, U.S. Government Identification Card, NSN 7540-00-926-8842, is available from General Services



CATHAL L. FLYNN

By direction

Distribution:

SNDL Part 1 (less 23B, 26LLL, 28E2, 29, 30, 31, 32, 35, 37, 40C, 40D, 41J, 42J1, 42J2, 45, 46, 50, 51 Annex A)

SNDL Part 2 (Naval Shore Activities) (Less A6, B, C1, C2, C5, C6, C7, C14, C15, FU1, V)

Copy to:

SNDL Part 1 (23B, 26LLL, 28E2, 29, 30, 31, 32, 35, 36, 37, 41J, 42J1, 42J2)

SNDL Part 2 A6 Headquarters U. S. Marine Corps
B (Special Agencies of the Department of Defense requiring direct distribution of Navy Publications and Directives)
C1 (Naval Personnel at Army Activities)
C2 (Naval Personnel at Air Force Activities)
C3 (Naval Personnel at DOD or other Government Agencies)
FU1 (Administrative Unit)

Stocked:

CO, NAVPUBFORMCEN

16 SEP 1985

Department of the Navy
Physical Security
and
Loss Prevention
Manual

Enclosure (1)

16 SEP 1985

TABLE OF CONTENTS

<u>CHAPTER 1 - INTRODUCTION</u>	<u>PAGE</u>
0100 - References and Guidance	1-1
0101 - Definitions	1-1
0102 - Purpose	1-6
0103 - Scope	1-6
0104 - The Security Problem	1-7
0105 - Security Responsibilities	1-7
0106 - Department of the Navy	1-7
0107 - Chief of Naval Operations	1-7
0108 - Commands, Bureaus and Offices	1-8
0109 - The Commanding Officer	1-8
0110 - The Security Officer	1-8
0111 - Duties of the Security Officer	1-9
0112 - The Security Manager	1-12
0113 - Organizational Relationships	1-12
0114 - The Physical Security Review Committee (PSRC)	1-12
Loss Prevention Sub-Committee (LPS)	1-13
Physical Security Review Board (PSRB)	1-14
0115 - Activity Upgrade Requirements/Waivers/Exceptions	1-14
0116 - New Construction	1-17
0117 - Facility Modifications	1-17

16 SEP 1985

CHAPTER 2 - SECURITY AND LOSS PREVENTION PLANNING

- 0200 - General
- 0201 - Physical Security Plan Format
- 0202 - Evaluation
- 0203 - Cost of Security
- 0204 - Coordination
- 0205 - Security Considerations
- 0206 - Calculated Risk
- 0207 - Crisis Situations
- 0208 - Sabotage
- 0209 - Terrorism
- 0210 - Threat Types
- 0211 - Security Plans
- 0212 - Physical Security Surveys
- 0213 - Threat Assessments

CHAPTER 3 - SECURITY AND LOSS PREVENTION MEASURES

- 0300 - Security Measures (definition)
- 0301 - Preventive and Protective Security Measures
- 0302 - Corrective Security Measures
- 0303 - Loss Prevention
 - Loss Analysis
 - Investigative and Police Resources
 - Loss Prevention Equipment
 - Employee Education
 - Discipline
 - Financial Responsibility
 - Claims
 - Criminal Prosecution

		<u>PAGE</u>
304	- Loss Reporting	3-4
	Accountability	3-5
	Investigation	3-6
	Summary Information	3-6
305	- Perimeter and Area Protection and Control	3-7
306	- Area Designation	3-8
	Restricted Areas	3-9
	Exclusion Area	3-9
	Limited Area	3-9
	Controlled Area	3-9
	Minimum Security Measures Required for Restricted Areas	3-10
	Non-Restricted Areas	3-13
307	- Signs and Posting of Boundaries	3-14
308	- Key Security and Lock Control	3-16
309	- Storage Containers, Vaults and Strongrooms	3-18
310	- Security Surveys and Inspections	3-18
311	- Security Checks	3-18
312	- Parking of Privately Owned Vehicles (POV)	3-19
313	- Traffic Control	3-19
314	- Security of Selected, Sensitive Inventory Items - Drugs, Drug Abuse Items and Precious Metals	3-20
315	- Security Requirements for "R" Coded Items at Base and Installation Supply Level or Higher	3-20
316	- Security Requirements for "Q" Coded Items at Base and Installation Supply Level or Higher	3-20

16 SEP 1985

		<u>PAGE</u>
0317	- Security Requirements for "R" and "Q" Coded Items below Base and Installation Level (i.e., small unit/individual supplies)	3-21
0318	- Security of Funds - Disbursing Office	3-21
0319	- Electric Typewriters, Calculators, Adding Machines, etc.	3-21
0320	- Video Recorders, Televisions, Film Projectors, Radio Receivers, etc.	3-21
0321	- Television (within lounges, quarters, etc.)	3-22

3 4 - THE SECURITY FORCE

	- General	4-1
0401	- Marine Corps Security Force (MCSF)	4-1
0402	- Functions of the Security Force	4-1
0403	- The Security Officer and the Security Force	4-2
0404	- Assignment of Security Officers	4-2
0405	- Size of Security Force	4-3
0406	- Legal Authority	4-3
0407	- Security Force Orders	4-3
0408	- Security Clearance for Security Force Personnel	4-4
0409	- Civilian Security Force	4-4
0410	- Determination of Security Force Strength	4-6
0411	- Determination of Posts	4-6
0412	- Types of Posts	4-6

16 SEP 1985

PAGE

413	- Post Requirements and Considerations	4-7
414	- Formula for Estimating Civilian Security Force Strength Requirements	4-8
415	- Supervisory Strength	4-10
416	- Military Armed Guards	4-10
417	- Augmentation of Security Force for Emergencies	4-10
418	- Crisis Response Force	4-10
	General	4-10
	Organization	4-10
	Size and Composition	4-11
	Command and Control	4-11
	Training	4-11
	Small Arms/Weapons/Equipment	4-12
419	- Police Forces	4-12

CHAPTER 5 - PERSONNEL AND VEHICLE MOVEMENT CONTROL

500	- General	5-1
501	- Purpose	5-1
502	- Personnel Identification and Movement Control System	5-1
503	- Identification and Control System Requirements	5-2
504	- Standard for Passes and Badges	5-3
	General	5-3
	Format/Characteristics	5-4
	Construction	5-5
505	- Personnel Identification and Control Procedures	5-5
	Regular Activity Personnel	5-5
	Visitors	5-6
	Contractor Employees	5-6
	Utility and Maintenance Personnel	5-6

OPNAVINST 5530.14A

16 SEP 1985

0506	- Application of Personnel Identification	5-
0507	- Enforcement of Movement Control	5-
0508	- Security Clearance on Badges	5-
0509	- Vehicle Identification and Movement Control	5-
	Regular Registration	5-
	Visitor Control	5-
	Commercial Vehicles	5-
	Control and Review of Identification	5-
	Media	5-
	Government-Owned Vehicles	5-
	Administrative Inspection of Vehicles	5-
	Honoring of Vehicle Identification	5-
0510	- Special Precautions	5-

CHAPTER 6 BARRIERS AND OPENINGS

0600	- The Purpose of Physical Barriers	6-
0601	- Types of Barriers	6-
0602	- General Considerations	6-
0603	- Fences	6-
	Chain Link Fencing	6-
	Alternative Fencing	6-
0604	- Walls	6-
0605	- Temporary Barriers	6-
0606	- Clear Zones	6-
0607	- Patrol Roads	6-
0608	- Inspection of Barriers	6-
0609	- Perimeter Openings	6-

16 SEP 1985

		<u>PAGE</u>
0610	- Gates	6-6
	Number and Location	6-6
	Inspection	6-7
	Pedestrian Gates	6-7
	Vehicular Gates	6-7
0611	- Doors, Windows, Skylights and Other Openings	6-7
0612	- Sewers, Culverts and Other Utility Openings	6-7
0613	- Utility Poles, Signboards and Trees	6-8
0614	- Vehicle Barriers	6-8

CHAPTER 7 - PROTECTIVE LIGHTING

0700	- General	7-1
0701	- Principles	7-1
0702	- Types of Protective Lighting Systems	7-2
0703	- Protective Lighting Parameters	7-3
0704	- Minimum Standards	7-3
0705	- Emergency Power	7-4
0706	- Technical Aspects	7-4
0707	- Protection - Control and Switches	7-5

CHAPTER 8 - INTRUSION DETECTION SYSTEMS

0800	- Introduction	8-1
0801	- Purpose	8-1
0802	- IDS Determination Factors	8-1
0803	- Types of Systems	8-2
0804	- IDS Description	8-3

OPNAVINST 5530.14A

16 SEP 1985

- 0805 - Sensor Subsystem
- 0806 - Data/Signal Transmission Subsystem
- 0807 - Annunciator, Control and Display Subsystem
- 0808 - Operating Power Subsystem
- 0809 - Interior Standards
- 0810 - Exterior Standards
- 0811 - Installation
- 0812 - Maintenance
- 0813 - Miscellaneous

CHAPTER 9 - PART ONE: SECURITY EDUCATION AND TRAINING

- 0900 - General
- 0901 - Security Education
 - Program Considerations
 - Program Formulation
 - Program Objectives
 - Educational Requirements
 - Graphic Media Aids
 - Indoctrination
 - Crime Prevention
 - Program of Instruction
 - Scheduling and Testing

- PART TWO: SECURITY FORCE TRAINING

- 0902 - General
- 0903 - Duties and Responsibilities
 - CNO (OP-009D)
 - Commanding Officers
 - Security Officers
 - Security Department Training Coordinators
 - Security Department Supervisors

16 SEP 1985

		<u>PAGE</u>
0904	- Scheduling Training	9-8
0905	- Evaluation of Training	9-8
0906	- Graduation Requirements	9-9
0907	- Field Training Officer	9-9
0908	- Recording Security/Law Enforcement Training	9-10
0909	- Emergency/Crisis Response Force Training	9-10
0910	- Emergency Vehicle Driver Training	9-10
0911	- Security and Law Enforcement Training Course	9-11
0912	- In-Service Training	9-13
0913	- Authority to Arm Security Force Personnel	9-14
0914	- Firearms Proficiency Training	9-15
	Training and Qualifications	9-15
	Annual Firearms Familiarization	9-15
	Quarterly Firearm Familiarization	9-15
	Nightfire Exercise	9-16
	Transition Course	9-16
	Failure to Qualify or Requalify	9-16
0915	- Conditions Under Which Security Force Personnel May Use Deadly Force	9-16
0916	- Additional Considerations Involving Firearms	9-17
0917	- Privately-Owned Weapons Prohibited	9-18
0918	- Contract Guard Training	9-18
0919	- Contract Guard Firearms Qualifications And Training	9-19

16 SEP 1985

CHAPTER 10 - SECURITY FORCE COMMUNICATIONS

1000	- General	10
1001	- Purpose	10
1002	- Types of Communications Systems	10
	Interior Communications	10
	Exterior Communications	10
1003	- General Requirement for the Use of Security Communications Systems	10

CHAPTER 11 - SECURITY DEVICES AND EQUIPMENT

1100	- General	11
1101	- Vehicles	11
1102	- Firearms and Ammunition for Security Forces	11
1103	- Guard Towers	11
1104	- Military Working Dogs (MWD)	11
1105	- Closed Circuit Television	11
1106	- Water Patrol Craft	11
1107	- Security Force Equipment	11
1108	- Security Force Individual Equipment	11

APPENDIX I References

APPENDIX II Bibliography

APPENDIX III Part 1 - Sabotage
 Part 2 - Espionage
 Part 3 - Bomb Threats

APPENDIX IV Pilferage/Larceny and its Prevention

APPENDIX V Legislative Jurisdiction and the Author
 Security Personnel

APPENDIX VI	Physical Security and the Posse Comitatus
APPENDIX VII	Physical Security Plan (Format)
APPENDIX VIII	Physical Security Survey Checklist
APPENDIX IX	Part 1 - Aviation Assets Part 2 - Navy Shipyards (CIA) Part 3 - Communication Stations Part 4 - Waterfront Security Part 5 - POL - Bulk Fuel Storage Areas
APPENDIX X	21 USC 1308 - Code of Federal Regulations (Extract)
APPENDIX XI	NAVCOMPT Manual, Vol. 4, Chap. 2, Paragraph 042351 (Disbursing Office Security)
APPENDIX XII	Intrusion Detection Systems
APPENDIX XIII	Minimum Training Standards for Security Force Personnel

CHAPTER 1

INTRODUCTION

0100. REFERENCES AND GUIDANCE

- a. Appendix I lists reference material cited in this manual.
- b. Appendix II provides a bibliography of security oriented reference publications.

0101. DEFINITIONS

For the purpose of this manual, the following definitions apply:

- a. Administrative Inspection. A cursory inspection of the contents of a vehicle with full consent of the operator or owner. Administrative inspections are conducted randomly, usually by members of the security force, with prior written authorization and direction by the installation/activity commander as to the methods and procedures to be employed. An administrative inspection is not to be confused with a probable cause search pursuant to a legal search warrant.
- b. Antiterrorism. Defensive measures to be used by the Department of Defense, its personnel, and their dependents, to prevent terrorist and unconventional acts.
- c. Armed Guard. A person equipped with a firearm whose primary function is to protect property and who has qualified with the firearm in an approved weapons qualification course. The guard is considered "armed" when the firearm and ammunition are readily available for immediate use.
- d. Concurrent Legislative Jurisdiction. Applies in those instances wherein in granting to the United States authority which would otherwise amount to exclusive legislative jurisdiction over an area, the State has reserved to itself the right to exercise, concurrently with the United States, all of the same authority. This shall be referred to as concurrent jurisdiction. (Refer to Appendix V for discussion on concurrent jurisdiction.)
- e. Counterterrorism. Offensive/reactive techniques taken to respond to terrorist acts, including the gathering of information and threat analyses in support of these measures. This manual is not concerned with counterterrorism.

f. Crisis Response Force. An installation/active force composed of security forces, military active duty personnel, on-board civil service personnel and other personnel, as appropriate; organized, equipped and trained to prevent mission disruption during civil disturbances or crises; to prevent, repel or contain overt attack by criminal elements and to help restore essential functions.

g. Espionage (against the United States). Espionage is overt, covert or clandestine activity designed to obtain information relating to the national defense with intent or reason to believe that it will be used to the injury of the United States or to the advantage of a foreign nation. (Pub 1) (For crimes of espionage, see title 18, United States Code, sections 792-799 (1976)). (Refer to Appendix III, for detailed discussion on espionage.)

h. Exclusive Legislative Jurisdiction. Situation wherein the Federal Government has received, by whatever method, all the authority of the State, with no reservation made to the State except of the right to serve process resulting from activities which occurred off the land involved. This shall be referred to as exclusive jurisdiction. (Refer to Appendix V for discussion on exclusive jurisdiction.)

i. Exception. A written and approved long-term (months or longer) or permanent deviation from a specific provision of this instruction. Long-term exceptions require interim compensatory security measures.

j. Facility. A facility is any building, structure or utility (including lines of communication and energy transmission) that is installed or established within a particular activity to serve a particular purpose.

k. Loss Prevention. Loss prevention is that part of an overall command security program dealing with resource measures and tactics devoted to care and protection of property on an installation. It includes identifying and reporting missing, lost, stolen, or recovered government property and developing trend analyses to plan and implement re-active and pro-active loss prevention measures.

l. Naval Activity. Any unit of the Naval Shore Establishment, of distinct identity which is established under a commander, commanding officer or an officer-in-charge by directive from appropriate authority.

m. Naval Installation. A naval installation consists of a grouping of two or more naval activities at a location.

16 SEP 1985

which one is responsible for the security of the perimeter which separates the grouping from non-naval areas and activities.

n. Partial Legislative Jurisdiction. Applies in those instances wherein the Federal Government has been granted for exercise by it over an area in a State certain of the State's authority, but where the State concerned has reserved to itself the right to exercise, by itself or concurrently with the United States, other authority more than the right to serve civil or criminal process in the area (e.g. the right to tax private property). This shall be referred to as partial jurisdiction. (Refer to Appendix V for discussion on partial jurisdiction.)

o. Physical Security. Physical security is that part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, materiel, and documents, and to safeguard them against espionage, sabotage, damage, and theft (JCS Pub 1).

p. Physical Security and Loss Prevention Program. The Physical Security and Loss Prevention Program is part of the overall security program at an activity. The physical security portion of the program is concerned with means and measures designed to fulfill antiterrorism matters, safeguard personnel and protect property by preventing, detecting, and confronting acts of unauthorized access, terrorism, espionage, sabotage, wrongful destruction, malicious damage, theft, pilferage, and other acts which would reduce to some degree the capability of the activity to perform its mission. Loss prevention is particularly concerned with preventing loss of supplies, tools, equipment or other materials in use, storage, transit and during the issue process. Concern is not only focused on the threat of criminal activity and acts of wrongdoing by forces external to the organizational unit. It is also specifically directed toward internal causes: theft and pilferage by those who have authorized access, inattention to physical security practices and procedures, and disregard for property controls and accountability. Physical security and loss prevention measures include instructions, procedures, plans, policies, agreements, systems and resources committed and designed to safeguard personnel, protect property, and prevent losses, thereby enhancing readiness.

q. Physical Security Review. An examination of the physical security and loss prevention programs of an activity to determine compliance with physical security policy. A physical security review is normally conducted by a

OPNAVINST 5530.14A
16 SEP 1985

r. Physical Security Survey. An in-house examination of the physical security and loss prevention programs of an activity to determine compliance with physical security policy. Survey results are not normally disseminated up the chain of command. They are used as a management tool by the surveyed command.

s. Property. Property consists of all: assets, including real property; facilities; funds and negotiable instruments; arms, ammunition and explosives; tools and equipment; materiel and supplies; computer hardware and software; and information in the form of documents and other media; whether categorized as routine or special, unclassified or classified, non-sensitive or sensitive, conventional or nuclear, critical, valuable or precious.

t. Proprietorial Interest Only. Applies in those instances where the Federal Government has acquired some right or title to an area in a State, but has not obtained any measure of the State's authority over the area. This shall be referred to as proprietorial jurisdiction. (Refer to Appendix V for discussion on proprietary jurisdiction).

u. Sabotage. Sabotage is an act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources. (JCS Pub 1). (For crimes of sabotage see title 18, United States Code, sections 2151-2157 (1976)). Note: During peacetime, destruction of government property, especially by U.S. military personnel, is normally investigated by the Naval Investigative Service as an act of wrongful destruction vice sabotage. For crimes against military property, see Article 108,. Uniform Code of Military Justice, or title 10, United States Code, section 908. (Refer to Appendix III, Part 1 for detailed discussion on sabotage.)

v. Security Force. That portion of a security organization at a Navy installation/activity comprised of either active duty military, DOD civilian police/guard or contract guard personnel, or a combination, tasked with providing physical security and law enforcement. The size and composition of the security force will depend largely on the size of the installation/activity, geographical location, criticality of assets, vulnerability and accessibility, as determined by the installation/activity commander.

w. Terrorism. The unlawful use or threatened use of force or violence by a revolutionary organization against individuals or property, with the intention of coercing or intimidating governments or societies, often for political or ideological purpose.

x. THREATCONS or threat conditions consist of a series of three color distinctions (White, Yellow and Red) describing progressive levels of terrorist threats to U. S. military facilities and personnel. Their prime purpose is to identify the various levels of terrorist threats and improve coordination and mutual support in antiterrorism activities. The progressive levels are as follows:

(1) THREATCON WHITE - Nonspecific threat of terrorism against Navy military and civilian personnel or facilities within a particular geographic area.

(2) THREATCON YELLOW - Specific threat of terrorism against Navy military and civilian personnel or facilities in a general geographic area.

(3) THREATCON RED - Imminent threat of terrorist acts against specific Navy military and civilian personnel or facilities.

y. Theft. Theft is a common name for larceny and pilferage. It is the taking of property without the owner's consent...with intent to deprive the owner of the value of the same, and to appropriate it to the use or benefit of the person taking (Black's Law Dictionary, Fifth Edition). Note: Under the Uniform Code of Military Justice, a distinction is made between larceny and wrongful appropriation. Larceny is taking with intent to permanently deprive the owner, whereas wrongful appropriation is taking with intent to temporarily deprive the owner. For crimes of larceny and wrongful appropriation, see Article 121, Uniform Code of Military Justice, or title 10, United States Code, section 921. (Refer to Appendix IV for detailed discussion on pilferage and its prevention.)

z. Waiver. A written temporary relief, normally not to exceed one year, from specific standards imposed by this instruction, pending actions or accomplishment of actions which will result in conformance with the standards required. Interim compensatory security measures are required.

0102. PURPOSE

To establish policy, and standardize guidance and requirements for physical security and loss prevention at Navy shore activities. Specifically, this manual:

- a. Establishes uniform minimum standards.
- b. Provides guidance for evaluating, planning and implementing each command's Physical Security and Loss Prevention Programs.
- c. Relates physical security measures to physical security interests.
- d. Provides a basis for determining cost effective physical security measures/upgrades through standardized practices.
- e. Assists those responsible for physical security in their efforts to carry out their assigned tasks.

0103. SCOPE

- a. This manual covers responsibilities for physical security and loss prevention. It classifies various security hazards, details protective measures and management actions which should and must be employed to provide an acceptable physical security posture, and selectively sets forth minimum physical security requirements. The language used is intended to separate recommended physical security measures from required measures. Words which are directive in nature (e.g., will, must, etc.) indicate that the physical security measure is mandatory.
- b. This manual applies to all Navy shore activities.
- c. This manual places specific emphasis on measures to assist in identifying, analyzing, reducing and eliminating losses of government property. Improvement of physical security within Navy shore activities is essential to loss prevention.
- d. This manual addresses physical security of resources and assets, and is intended to cover matters not covered by other specialized security programs. Protection of classified material, sensitive compartmented information (SCI), automated data processing (ADP) systems, nuclear weapons, and sensitive conventional arms, ammunition and explosives (AA&E) are specifically addressed in references (a) through (e).

e. This manual is not concerned with counterterrorism.

f. Compatibility of physical security requirements and the elimination of conflicting guidance are primary objectives. The Physical Security and Loss Prevention Program addresses the protection of personnel and property. Such protection is accomplished by identifying the property requiring protection, assessing the threat, committing resources, determining jurisdiction and boundaries; by establishing perimeters, barriers, and access control; by providing the means to detect efforts to wrongfully remove, damage or destroy property; and by employing a security force sufficient to protect, react to and confront situations and circumstances which threaten personnel and property. When property has special characteristics, such as when it is classified or sensitive, additional physical security requirements are levied by other specialized programs as earlier indicated. Those requirements augment, and are in addition to, any basic guidance provided by this instruction.

0104. THE SECURITY PROBLEM

The security problem is influenced by the mission of the activity, the type and jurisdiction of the property, the geographic location and size of the activity, the topography of the area, the economic and political atmosphere, potential and existing threats, and the logistical and operational support provided by other organizations.

0105. SECURITY RESPONSIBILITIES

Security is the direct, immediate and moral responsibility of all persons in the naval service and civilians employed by the Navy. Specific responsibilities are set forth in the following articles.

0106. DEPARTMENT OF THE NAVY

The Department of the Navy is responsible for ensuring that the degree of security for all naval assets is commensurate with the requirements of the Department of Defense (DOD).

0107. CHIEF OF NAVAL OPERATIONS

The Chief of Naval Operations (CNO) is responsible for the formulation and dissemination of Navy policies relating to security, and for supervision and coordination of their implementation.

0108. COMMANDS, BUREAUS AND OFFICES

The command, bureau or office having authority over an activity provides the means to the activity for physical security implementation. This is accomplished through the exercise of executive authority, procedures, inspections, staffing, funds, materials, facilities and technical direction.

0109. THE COMMANDING OFFICER

The commanding officer of an activity is responsible for physical security at that activity, for appointing a security officer, and for establishing and maintaining a physical security and loss prevention program within the activity. The commanding officer of an installation is responsible for installation perimeter security, or for coordination thereof. The commanding officer will provide sufficient resources, staff assistance and authority to the security officer to implement, manage and execute an effective physical security and loss prevention program. Appendix VI discusses commanding officers' responsibility and authority relevant to protection of naval installations and activities.

0110. THE SECURITY OFFICER

The commanding officer or officer in charge of each naval activity will appoint a security officer. The basic function of the security officer is to assist the commanding officer by determining the adequacy of the command Physical Security and Loss Prevention Program, by identifying to the commanding officer those areas in which improved physical security and loss prevention measures are required, and by managing the program.

The security officer will:

a. Be a fully trained and qualified (experience and training primarily in the law enforcement, physical security or loss prevention areas) civilian security specialist GS/GM-080-11 or above, or a naval officer/warrant officer with equivalent physical security experience, when either of the following criteria is met:

(1) The command or activity has a mission requiring complex and comprehensive physical security systems and resources.

(2) The command or activity has more than 300 military or civilian personnel assigned or employed.

16 SEP 1985

Activities whose security programs, size and scope do not meet any of the above criteria may designate a civilian employee GS-080-7 or above, senior enlisted personnel E7 or above, or a naval officer/warrant officer with any designator to be the security officer.

b. Be designated in writing by the commanding officer or officer in charge and be identified by name to all members of the command who are assigned primary or collateral security duties.

c. Be familiar with the provisions of this instruction.

d. Be provided sufficient training, resources, staff assistance and authority to manage and carry out an effective Physical Security and Loss Prevention Program.

0111. DUTIES OF THE SECURITY OFFICER

The security officer will:

a. Manage, implement and direct the command's physical security, antiterrorism and loss prevention programs, to include developing and maintaining comprehensive physical security instructions and regulations.

b. Determine adequacy of the command's physical security, antiterrorism and loss prevention programs, identify those areas in which improvements are required, and provide recommendations for such improvements to the commanding officer.

c. Develop and maintain a current command Physical Security Plan.

d. Conduct physical security surveys, inspections, and audits.

e. Identify the real property and structures to be protected.

f. Identify restricted areas and ensure the areas are properly designated by the commanding officer, as appropriate.

g. Identify by location and priority the assets to be protected.

h. Determine boundaries and establish perimeters of such areas.

i. Determine, in coordination with the staff legal officer and facilities engineer, legal legislative jurisdiction of all areas, including maintenance of an installation map depicting precise jurisdictional boundaries.

j. Assess the threat to such areas.

k. Determine and identify the necessary resources (i.e., funds, staff, equipment, etc.) to implement effective Physical Security and Loss Prevention Programs.

l. Recognize constraints in resource application.

m. Determine and recommend establishment of barriers and points of ingress and egress.

n. Develop and maintain the personnel identification and access control system(s).

o. Coordinate security requirements of tenant activities and ensure that those requirements are entered in applicable host-tenant agreements and inter/intra-service support agreements (ISSA).

p. Provide technical assistance on all security matters.

q. Ensure liaison is maintained with Federal and civil agencies, host country officials or military activities concerning mutual security responsibilities.

r. Develop security and antiterrorism aspects of crisis management. Participate in the planning, direction, coordination and implementation of procedures for crisis management of situations (including hostage situations) which pose a threat to the physical security of the command. Act as the commanding officer's crisis manager and primary staff advisor during any security related crisis.

s. Identify physical security procedures and equipment that will detect and/or prevent wrongful removal, damage, destruction or compromise of protected property.

t. Identify other physical security measures and procedures necessary to accomplish the command's mission.

u. Establish and provide for maintenance of records relating to losses of government and personal property, violations and breaches (including indications thereof) of

16 SEP 1985

physical security measures and procedures, including corrective action(s) taken. These records shall be retained until completion of the cognizant Inspector General command inspection cycle, or a minimum of two years, whichever is greater.

v. Act as command's point of contact for coordinating and monitoring physical security waivers and exceptions.

w. Establish and maintain liaison and working relationships and agreements with Federal investigative agencies, local Naval Investigative Service components, state and local law enforcement and fire protection authorities (in the absence of a command fire prevention and protection function).

x. Serve as facilitator of, and be responsible for, minutes and records of the command Physical Security Review Committee.

y. Maintain regular contact and collaborate with managers of specialized security programs within the command concerning physical security threats and requirements.

z. Maintaining contact with and soliciting advice (when appropriate) from the cognizant staff judge advocate concerning the legal aspects of physical security.

aa. Maintaining regular contact with the OPNAV mission sponsors of the counterterrorist program.

bb. Develop, maintain, and administer an ongoing employee physical security and loss prevention education awareness program.

cc. Develop and maintain a command Loss Prevention Program and supporting loss prevention plan which:

(1) Identifies and prioritizes, by attractive nature and likelihood of loss, assigned property susceptible to theft and pilferage.

(2) Identifies command property accountability, inventory, causative research and inspection procedures in effect. Makes recommendations to the commanding officer, as appropriate.

(3) Establishes procedures for adequate internal and external investigative measures, and the review and trend analysis of losses.

(4) Establishes command functional areas and designates personnel to be active in and responsible for loss

reporting, review, trend analysis, and investigative requests and liaison.

(5) Establishes procedures for ensuring that all losses and gains, inventory adjustments, and surveys of property are reported in accordance with reference (f).

(6) Monitors legal, disciplinary and administrative procedures and remedies applicable to those found responsible and liable for losses.

0112. THE SECURITY MANAGER

The security manager's function differs from that of the security officer. The security manager is the commanding officer's advisor and direct representative in matters pertaining to security of classified material. In the performance of these duties, he/she is guided by reference (a). The security officer operates in support of the security manager in protecting classified material.

0113. ORGANIZATIONAL RELATIONSHIPS

The security officer reports directly to the commanding officer, or via the executive officer to the commanding officer, in the performance of assigned duties. He/she collaborates with officers or managers of other specialized security programs within the command concerning physical security needs, threats, requirements and implementation. The security officer may also serve as the security manager, or manager of other specialized security programs or vice versa. Occasionally, the security officer function may be a collateral duty, depending upon the size of the activity.

0114. THE PHYSICAL SECURITY REVIEW COMMITTEE (PSRC)

a. Responsibilities. The commanding officer of a naval installation will designate in writing a Physical Security Review Committee (PSRC) to advise and assist in applying the standards of and implementing the program for physical security and loss prevention set forth in this and other pertinent directives. The committee will:

(1) Assist in determining requirements for and evaluating security afforded to areas of the activity or installation and its tenant activities.

(2) Advise on establishment of security areas.

(3) Review the draft physical security and loss prevention plan, or recommended changes thereto, prior to submission to the commanding officer.

16 SEP 1985

(4) Review reports of significant losses and breaches of security, and based on analysis of such instances, recommend improvements to the Physical Security and Loss Prevention Program.

b. Membership. The PSRC will, as a minimum, include the following membership (if so staffed):

(1) Executive officer (chairperson). (Activities with a flag officer as second in charge may appoint an O-6 or civilian equivalent to act as chairperson).

(2) Security officer.

(3) Comptroller.

(4) Security manager and officers or managers of other specialized security programs (i.e. base/activity police chief, Marine barracks commanding officer, ADP security officer, etc.).

(5) Public works officer and/or facilities manager.

(6) Supply officer.

(7) Legal officer and/or general counsel.

(8) Directors/heads of activity/installation and major command functions whose missions are influenced and impacted by security requirements.

(9) Senior rated master-at-arms, or senior designated master-at-arms, assigned physical security duties.

(10) Internal review functional manager.

(11) Weapons officer.

c. Naval Investigative Service. Representative(s) of the Naval Investigative Service, while not listed in the required membership, may be included.

d. Meetings and Minutes. Committee members or their representatives will meet as required, but at least quarterly. Minutes of the meeting will be made a matter of record and such records will be retained until completion of the cognizant Inspector General command inspection cycle.

e. Loss Prevention Subcommittee (LPS). The chairperson will appoint a Loss Prevention Subcommittee (LPS) which will be required to meet at least quarterly to review and tabulate

losses and action taken or pending. Meeting summaries will be appended to PSRC quarterly minutes. Internal review participation in the LPS is required (if so staffed). At least three PSRC members (including internal review participation) will be appointed to serve on the LPS.

f. Physical Security Review Board. The commanding officer of a naval installation will formally establish a Physical Security Review Board with goals and purpose similar to that of the activity Physical Security Review Committee. Membership will include representatives of each tenant activity located on the premises of the installation. The PSRB will meet at least annually. A specific goal of the board is coordination of mutually supportive physical security and loss prevention practices.

0115. ACTIVITY UPGRADE REQUIREMENTS/WAIVERS/EXCEPTIONS

All activities will review their existing security posture and determine modifications necessary to conform to this instruction. A Plan of Action and Milestones (POA&M) will be developed to correct discrepancies. Deviations which are not correctable within 12 months will be covered by an approved waiver or exception pending completion of the required upgrade effort. Operational procedures will be implemented as soon as possible.

a. Waivers. Requests for waiver of specific requirements will be submitted to the activity's/installation's major claimant (initial waiver authority may be delegated by the FLTCINCs to type commands). Echelon two commanders may approve initial waivers for their own headquarters but must forward waiver extension requests to CNO (OP-09N). The request for waiver must include a complete description of the problem and compensatory measures/alternative procedures, as appropriate. Approved waivers will exempt the recipient from a specific security standard for a period of twelve months. Extension of the waiver for an additional twelve months must be forwarded via the chain of command and approved by OP-09N. Further 12-month incremental extensions for the same waiver must also be approved by OP-09N.

b. Exceptions. Requests for exceptions to specific requirements due to permanent or long-term (more than 36 months) inability to meet a security standard must be forwarded via the chain of command to OP-09N for approval. Each exception request will include a comprehensive study of the problem and describe compensatory measures and procedures to be employed. Exception requests will be reviewed and approved by physical security and command elements at all echelons.

16 SEP 1985

c. Waivers and exceptions to references (a) through (e) security criteria fulfill the waiver and exception requirements of this instruction.

d. It is recognized that in other countries the host nation may have ultimate responsibility for certain aspects of security, such as perimeter security for naval activities located there, and that Navy authorities may resultingly be constrained in the implementation of certain requirements set forth in this instruction. In those instances, the activity concerned must request waivers/exceptions from compliance with requirements which conflict with local prohibitions and conditions. It is also recognized that certain naval activities, because of other circumstances or small complement, may be unable to conform to certain requirements set forth herein. However, requests for such exceptions will be submitted in accordance with procedures set forth in this instruction.

e. Waiver and Exception Requests. The initiating command will assign a waiver or exception number in accordance with sub-paragraphs f and g below. All information requested below must be provided in waiver, waiver extension, and exception (permanent and long-term) requests. Requests will be in letter format, and all elements of sub-paragraphs f and g will be specifically addressed. Non-applicable elements shall be noted as "N/A".

f. Waiver and Exception Format. This paragraph provides guidance for the assignment of waiver or exception numbers (or waiver extensions) for deviations from established physical security standards. The basic objective is to provide a ready identification of any given waiver or exception (or waiver extension) with respect to the activity involved, year of issuance, and modification status. Each waiver, exception, or waiver extension must be identified as follows:

(1) The first five digits represent the unit identification code (UIC) of the activity initiating the request.

(2) The next digit is either "W" for waiver or "E" for exception.

(3) The next two digits represent the serial number of the request, beginning with 01.

(4) The last two digits identify the calendar year of the request.

16 SEP 1985

(5) Example:

01234-W01-84

UIC= 01234

W = Waiver ("E" for exception)

01 = 1st waiver request of calendar year

84 = 1984

g. The following format is prescribed for requests for waivers:

(1) Line 1 - Waiver number.

(2) Line 2 - Statement of the waiver requirement and references to the Chapter, section, and paragraph in this instruction which cites the standards which cannot be met.

(3) Line 3 - Specific description of the conditions which caused the need for the waiver and reasons why the standards in this instruction cannot be met.

(4) Line 4 - Generic description of the material affected by the waiver request.

(5) Line 5 - Description of the physical location of affected facilities or area. Identify structures individually by building number.

(6) Line 6 - Identify interim mandatory compensatory measures in effect or planned.

(7) Line 7 - Describe the impact on mission and any problems which will interfere with safety or operating requirements if the waiver is not approved.

(8) Line 8 - Identify resources, including estimated cost, to eliminate the waiver and estimated cost.

(9) Line 9 - Identify actions initiated or planned (e.g., local capability or other) to eliminate the waiver and estimated time to complete.

h. The following format is prescribed for requests for exceptions:

(1) Line 1 - Exception number.

(2) Line 2 - Statement of the exception requirement and reference to the chapter, section, and paragraph in this instruction which cites the standards which cannot be met.

(3) Line 3 - Specific description of the conditions which caused the need for the exception and reasons why the standards in this instruction cannot be met.

(4) Line 4 - Generic description of the material affected by the exception request.

(5) Line 5 - Description of the physical location of affected facilities or area. Identify structures individually by building number.

(6) Line 6 - Identify in detail equivalent security measures which are being applied.

(7) Line 7 - Describe the impact on mission and any problems which will interfere with safety or operating requirements if the exception is not approved.

i. Long-term exception requests must provide the information set forth in paragraph 0116g.

0116. NEW CONSTRUCTION

New construction shall comply with the requirements of this instruction. Plans for new construction, incorporating physical security features, shall be reviewed by the security officer or designated representative during the design process and various review phases.

0117. FACILITY MODIFICATIONS

Physical security enhancement modifications (new intrusion detection alarm system equipment, security fencing, security lighting, etc.) to existing buildings, facilities, sites, etc., shall be reviewed by the security officer or designated representative during the design process and review stages.

16 SEP 1985

CHAPTER 2

SECURITY AND LOSS PREVENTION PLANNING0200. GENERAL

Security planning is a constant process carried out both in advance of security operations and concurrently with them. Normally, planning for any type security operation will fall within the patterns used by most military planners; i.e., the estimate, the plan, and its implementation in the administrative plan or annexes. The security estimate (with its analysis of the mission) and situation (courses of action and decision) provides the basis for the security plan. Each naval activity/installation will develop and publish a physical security plan and a loss prevention plan, as set forth in Chapter 1. The physical security plan will contain standard operating procedures which detail required crisis management actions with separate annexes for fires, explosions, civil disturbances, major accidents, hostage situations, sabotage, bomb threat incidents, terrorist acts, natural disasters and other potential crises as appropriate. Physical security plans for tenant activities on a naval installation will be integrated into the installation physical security plan.

0201. PHYSICAL SECURITY PLAN FORMAT

A model Physical Security Plan format is found in Appendix VII. The activity/installation physical security plan, however, should be written in a format most applicable to the authorizing command. For small tenant commands, a chapter in the Staff Regulations which discusses the command's PSRC, defines access controls and restricted areas, establishes a lock and key control program and loss prevention program, and implements the security plan of the host command may suffice. For moderate size activities and large tenant commands, a letter type directive with enclosures addressing specialized subjects such as crisis management, security during THREATCONS, loss prevention, access control procedures, emergency responses, may be adequate, particularly if well integrated with a comprehensive disaster preparedness instruction. For large installations a security plan written as a Manual (with annexes and appendices) may be more appropriate. Regardless of the format, the plan must be a "users" instruction focused on clearly delineating how the command conducts day-to-day security and how it responds to security incidents. It should not be philosophical or a verbatim reiteration of this manual, but instead reflect the detailed implementation of Navy policy at the activity/installation level.

16 SEP 1985

0202. EVALUATION

In evaluating the need for and the type and extent of physical protection required at an activity, the following factors, among others, must be considered in planning:

a. Overall importance/criticality of the command.

(1) Mission and sensitivity of the activity.

(2) Importance of the activity to the continuity of essential naval operations.

b. Overall susceptibility/vulnerability of the command to threats.

(1) The threat to a specific command as defined by military intelligence and investigative agencies.

(2) Ease of access to vital equipment and materials.

(3) Location, size, deployment, and vulnerability of facilities within the activity and the number of personnel involved.

(4) Need for tailoring security measures to mission critical operating constraints and other local considerations.

(5) Probable duration of operations.

(6) Geographic location (provides or does not provide natural barriers).

(7) Legal jurisdiction of real property.

(8) Mutual aid agreements and unilateral assistance agreements.

(9) Local political climate.

(10) Adequacy of storage facilities for valuable or sensitive material, including precious metals, drugs and arms, ammunition and explosives.

(11) Accessibility of the activity to disruptive, criminal, subversive, or terrorist elements.

(12) Possible losses and their impact on command mission and readiness.

16 SEP 1985

(13) Possibility or probability of expansion, curtailment or other changes in operation.

(14) Overall cost of security.

(15) Availability of personnel and material.

(16) Coordination of security forces.

(17) Calculated risk.

(18) Potential for increase in threat.

c. ADP risk assessments contained in reference (c) should be reviewed to help determine susceptibility of the command to various threats.

0203. COST OF SECURITY

Physical security cost expenditures should generally be based on the cost of the item to be protected, possible damage which loss of the item could inflict upon the civilian population and importance of the item to overall national security and Navy readiness. The cost of security is frequently greater than the dollar value of the property/material. Sensitive items which may be a threat to the civilian population or vital to national security will be provided additional security commensurate with their sensitivity and the threat to their security.

0204. COORDINATION

Physical security of separate activities and installations will be coordinated with other military activities/installations in the immediate geographical area and local civilian law enforcement agencies or host government representatives. Within the physical confines of the activity, the host activity shall coordinate physical security measures employed by all tenant activities, regardless of the military command or service represented. The physical security of all arms, ammunition and explosives, and other hazardous material held by tenant activities will be closely coordinated with the host activity. All planning that may result in the physical relocation of an organizational element, physical changes to a facility or a realignment of functions will include the security officer from the outset to ensure that security considerations are included during initial planning.

0205. SECURITY CONSIDERATIONS

Security measures to be considered when developing physical security plans are:

- a. Personnel screening and indoctrination.
- b. Protection for vulnerable points/assets within the activity.
- c. Security force organization and training.
- d. Personnel identification and control systems.
- e. Installation of physical security hardware (e.g., intrusion detection systems, barriers, access control systems).
- f. Key and lock control.
- g. Coordination with other security agencies.

0206. CALCULATED RISK

Calculated risk is the concept which dictates that when there are limited resources available for protection, possible loss or damage to some supplies or to a portion of the activity is risked in order to ensure a greater degree of security to the remaining supplies or portions of the activity. For example, precious metals should be given protection priority over less valuable property items. However, security controls shall not be relaxed to the degree that controls for less valuable items are disregarded and accountability lost.

0207. CRISIS SITUATIONS

In evaluating the need for and extent of physical protection required, the possibility of injury to security force personnel must be considered. This is especially relevant when addressing security measures taken during crisis situations (e.g., bomb threats, fires, terrorist incidents or natural catastrophes) to control government assets; to limit damage and provide emergency services for containment of the incident to restore the target activity to normal operation. Situations which present unique and growing physical security problems are the handling of bomb threats and terrorist incident as well as any change in threat conditions (THREATCONS) (see paragraph 0211). Bomb threat situation planning should be coordinated and cross-referenced with the command disaster preparedness plan and include preventive measures to reduce the opportunities for introduction of bombs; procedures for evaluating and handling threatening messages; policy on evacuation and safety of personnel; procedures for search; procedures for obtaining assistance and support of law enforcement and military explosive ordnance disposal (EOD) units; procedures in the event a bomb is found on premises and procedures to be followed in the event of an explosion or detonation (refer to Appendix III Part 3 for a discussion on bomb threats).

16 SEP 1985

0208. SABOTAGE

Sabotage is defined in Chapter 1 and discussed in Part 1 of Appendix III. If successfully carried out, such acts can cause destruction equal to acts of war but without fear of retaliation against the hostile nation's warmaking capability. Such acts can inhibit scientific and technological progress, impair the effectiveness of a nation's foreign policy and initiate or increase domestic unrest. Additionally, it must be assumed that an outbreak of hostilities against this country would probably be preceded by efforts to sabotage the ability of the United States to defend itself. To this end, commanders at every level must take action to counter this threat.

a. Countersabotage Methods. As a minimum measure, assigned personnel should be made aware by local investigative/intelligence organizations of the nature of the threat posed by anti-military individuals and groups. Active liaison with the Naval Investigative Service is a major factor in obtaining such information at the local level. To help minimize the threat of sabotage, the physical security measures delineated will be implemented and strict access control/visitation privileges must be observed aboard Navy installations.

0209. TERRORISM

Terrorism is the unlawful use of threatened use of force or violence by a revolutionary organization against individuals or property, with the intention of coercing or intimidating governments or societies often for political or ideological purposes. Terrorism in the United States is increasing. Acts of terrorism directed at naval personnel, activities or installations have the potential to destroy critical facilities, injure or kill personnel, impair or delay accomplishment of mission and cause incalculable damage through adverse publicity and public perceptions of incident handling and results. Guidance for responding to terrorists acts overseas is contained in reference (s).

a. Antiterrorism Organization. The most cost effective, broadly based method of organizing an antiterrorism effort is to integrate it as much as possible with crisis management procedures set up to prevent, control, contain or restore other natural and man-made crises. Essentially, specific anti-terrorism planning involves two defenses to be established in an effort to prevent terrorist acts.

16 SEP 1985

(1) Intelligence. Adequate information obtained through threat assessment and continuing contacts with the Naval Investigative Service are essential to prepare for or forestall a terrorist incident.

(2) Target Hardening and Procedural Safeguards. Physical security measures established to protect critical and sensitive activity assets against terrorist (or other) threats must be sufficient to increase the costs and risks to the more dedicated professional terrorist.

b. Terrorist Methods. The record of terrorist activities directed at military activities indicates that the following methods might be employed:

(1) Bombs. Bomb(s) used may be of any degree of sophistication and may be placed to destroy equipment, cause fires, create casualties, etc. Depending on the bomb(s) size and placement, the impact may range from a minor to a major crisis.

(2) Ambush. Rapid ambush attacks by individuals or small groups to assassinate individuals, eliminate groups of naval personnel or destroy/steal assets in remote locations on the installation or in transit.

(3) Armed Attack. An armed assault usually with one or more diversionary actions carried out by small groups against key personnel or critical assets on an installation with the objective of causing disruption of mission activities and creating adverse publicity. Hostage taking is not a usual tactic in this type of terrorist action unless the attackers are prevented from escaping.

(4) Hostage Situations. A terrorist group may undertake the seizure of a specific hostage for ransom or political bargaining purposes. An armed attack scenario may be used to seize a critical asset (ship, submarine, aircraft, etc.) when personnel are present in order to use both the asset and the personnel as leverage to bargain for publicity and political advantage. This type of crisis incident directed at a naval activity could rapidly escalate to include government crisis management overview at the highest levels. Care must be taken to provide for this possibility in antiterrorism planning. Each activity will ensure that physical security plans include captor/hostage situation procedures. The Naval Investigative Service can provide assistance.

(5) Sabotage. Terrorist groups may engage in the use of various sabotage methods described in Appendix III, Part 1 in order to harass and enervate security forces.

16 SEP 1985

0210. THREAT TYPES

a. The following categories of threats have been established which describe the various individuals or groups of individuals that activities must be aware of in order to establish adequate security countermeasures against particular kinds of crisis situations:

(1) Threat Type ONE. One or more outsiders (non-government persons) who seek access to a base/restricted area/assets in which to perform an unauthorized act (i.e., vandalism, theft, etc.).

(2) Threat Type TWO. An individual or group, authorized access to a base/restricted area/asset, seeking to steal/remove an item of government property from the installation.

(3) Threat Type THREE. A disgruntled employee seeking to perform an act of sabotage or otherwise destroy government property or impair mission accomplishment.

(4) Threat Type FOUR. An individual (outsider) or group seeking to make a political statement (anti-military, anti-defense, anti-nuclear, etc.), usually non-violent in nature, and seeking to embarrass the Navy by causing adverse publicity.

(5) Threat Type FIVE. An individual (outsider), terrorist in philosophy and action, seeking access to a naval installation for the purpose of perpetrating an act of violence (sabotage, bombing, hostage abduction, murder, arson, theft of sensitive matter: nuclear weapons, conventional arms, ammunition and explosives, etc.).

(6) Threat Type SIX. A 2-12 person group of well-armed, well-trained dedicated terrorists seeking access to a naval installation for the purpose of perpetrating an act of violence (sabotage, bombing, hostage abduction, murder, arson, theft of sensitive matter: nuclear weapons, conventional arms, ammunition, explosives, etc.).

b. Protection Criteria. The matrix contained in Table 2-1 summarizes many of the Navy's more sensitive areas and assets and those threat types commanding officers must have the ability to counter. Commanding Officers must have contingency plans to counter threats as indicated:

16 SEP 1985

AREAS

	<u>COMMANDING OFFICERS MUST HAVE</u> <u>ABILITY TO COUNTER THREATS</u>					
	1	2	3	4	5	
Bases	1	2	3	4	5	
Shipyards	1	2	3	4	5	
Aviation Areas	1	2	3	4	5	
Waterfronts	1	2	3	4	5	
Nuclear Weapons Storage	1	2	3	4	5	6
Communications Facilities	1	2	3	4	5	
Intelligence Collection/ Sensitive Communication Sites	1	2	3	4	5	
Conventional Arms, Ammunition and Explosives Storage Sites	1	2	3	4	5	
Bulk POL (ground Fuels, POL war reserve, etc.)	1	2	3	4		

ASSETS

Small Arms (Armories)	1	2	3	4	5
Supply Items	1	2	3	4	5
Funds and Negotiable Instruments	1	2	3		
Drugs, Drug Abuse Items	1	2	3	4	
Precious Metals	1	2	3		
Classified Information/Material	1	2	3	4	
ADP Facilities	1	2	3	4	

TABLE 2-1

0211. SECURITY PLANS

a. Local orders/directives will be written to cover all phases of security operations. They will be disseminated to all persons with a need-to-know and who are charged with security responsibilities. Such orders/directives must provide instruction relative to the individual's security responsibility, authority and the procedures for handling and reporting incidents. These orders/directives must be kept current and reflect the routine needs of the command as well as any unusual situation that requires special security measures.

b. Contingency plans for major shore commands and their senior commands exercising territorial authority shall contain provisions for reinforcement of security forces, when necessary.

c. Tenant commands will comply with host activity physical security requirements. Tenant commands will develop and maintain a physical security plan for their activities using guidelines set forth in support of the host commands physical security plan. These plans will be coordinated with host command security officers.

16 SEP 1985

d. Tenant and host commands, as appropriate, will ensure tenant/host and intra- or inter-service support agreements outline complete and detailed physical security requirement responsibilities.

e. Orders and contingency plans must consider recommended actions at various terrorist threat condition levels (THREATCONS) defined in paragraph 0101w.

0212. PHYSICAL SECURITY SURVEYS

a. A physical security survey differs from an inspection review in that a survey covers an in-house formal assessment of an activity. Each survey includes a complete reconnaissance, study analysis of the physical security of each installation's property and its operation. These surveys are designed to show the commanding officer what security measures are in effect, what areas need improvement, and provide a basis for determining priorities for funding/work accomplishment.

b. The security officer at each activity shall conduct a physical security survey at least annually. Appendix VIII to this instruction shall be used as a guide, but is not meant to be all-inclusive.

c. Results of physical security surveys will be retained until completion of the cognizant Inspector General command inspection or a minimum of two years, whichever is greater.

0213. THREAT ASSESSMENTS

a. Based on available information which can be legally obtained, the command must determine the active short, medium, and long-term threat. The Naval Investigative Service can supply the threat evaluations on request. Such information must be carefully analyzed to determine what additional physical security measures are necessary where physical security requirements are not adequate. The possibility of attempts by terrorist groups, criminals, activists, and hostile intelligence operatives to penetrate the security of military installations continues to be a matter of serious concern within the Department of Defense and high levels of government. Accordingly, the Naval Investigative Service will provide an annual area threat assessment through the local Naval Investigative Service Resident Agency responsible for counterintelligence support for the activity concerned upon request.

b. All Naval Investigative Service components routinely maintain close and effective liaison with the Federal Bureau of Investigation and other appropriate federal, state and local law enforcement and intelligence agencies and disseminate, by the most

expeditious means, known threat information affecting the security of a particular military installation. If a command independently detects or perceives threat information, the servicing Naval Investigative Service component shall be promptly notified so that appropriate Naval Investigative Service follow-up action may be initiated. Follow-up action will generally consist of the Naval Investigative Service component attempting to obtain amplifying details/intelligence regarding the perceived threat.

c. The Naval Investigative Service provides annual up-to-date counterintelligence and criminal information for over 182 foreign ports listed in the classified supplements to the Port Directories produced by the Fleet Intelligence Centers. Commanders of military installations located in foreign countries may utilize the classified supplements to assist in satisfying the threat assessment requirements of this instruction as well as assistance from the Naval Investigative Service.

16 SEP 1985

CHAPTER 3

SECURITY AND LOSS PREVENTION MEASURES0300. SECURITY MEASURES

Security and loss prevention measures are actions taken to establish or maintain an adequate physical security and loss prevention posture for a command.

0301. PREVENTION AND PROTECTIVE SECURITY MEASURES

Collectively, security measures create conditions favorable to the maintenance of an effective security posture. They are designed to develop habits and attitudes conducive to the maintenance of good security practices and the elimination of existing/potential causes of security breaches and violations.

0302. CORRECTIVE SECURITY MEASURES

These measures deal with breaches of security. They correct conditions that might lead to further security breaches and include, but are not limited to:

- a. Identification and/or apprehension of security violators.
- b. Investigation, analysis and reporting losses.
- c. Disciplinary and/or, administrative personnel action.

0303. LOSS PREVENTION

A vigorous loss prevention program is essential at every Navy command. Losses of property may prevent timely accomplishment of mission requirements and cost millions of dollars annually. Losses must be minimized by the application of a comprehensive loss prevention program consisting of: loss analysis, proper use of available investigative and police resources, continuing employee loss prevention education, the application of firm corrective measures, administrative personnel actions and pursuit of prosecution, and other loss prevention measures where necessary. These topics will be addressed during required meetings of the activity's Physical Security Review Committee. As a minimum, loss prevention measures will consist of the following:

- a. Loss Analysis. To help identify trends and patterns of losses and gains, all incidents involving reportable property must be included in an ongoing program of analysis. A continuing loss analysis process should consider

the types of material lost; geographic location; supply system Master Stock Inventory Record (MSIR) locations; times and dates; proximity of specific personnel; proximity of doorways, passageways, loading docks/ramps, gates, parking facilities, piers and other activities adjacent to loss/gain locations; material movement paths; material condition codes; and the number and distribution of MSIR locations used for remaining like property. At activities where there are extensive losses, accomplishment of the loss analysis process may require application of data processing resources to adequately sort and analyze essential factors. Resulting analyses of loss/gain trends and patterns will be used to balance the allocation of resources available for crime prevention. Reference (f) establishes procedures for reporting and processing information.

b. Investigative and Police Resources. To prevent or reduce losses of government property, it is essential that supply centers, naval shipyards, ordnance stock points, naval stations and similar naval activities assign available investigative and police personnel to loss prevention functions. Patrols of pilferable or property areas should be stressed and a preliminary investigative capability should exist during all working production shifts (especially night shifts). Local loss analysis program data should be used to program security resources to combat losses. Shore activities which are tenants at an activity and lack police or investigative resources should include loss prevention support in the written host-tenant agreement or inter-service support agreement (ISSA) with the host or responsible command. For shore activities located outside military installations which cannot obtain loss prevention support from a military host or responsible activity, a written mutual support agreement for obtainable services should be pursued with the local civilian law enforcement agency having criminal jurisdiction.

c. Loss Prevention Equipment. Exterior doors in warehouses, storage buildings, office buildings and other structures which contain high value, sensitive, or pilferable property, supplies, or office equipment will be afforded security protection commensurate with the value and sensitivity of the structure's contents. At a minimum, hinges will either be non-removable or be provided with inside hinge protection which prevents locked doors opening even if hinges are removed, and lock/hasp security systems that meet Military Specification (MILSPEC) Standards for the structure's contents. Built-in dial type Group One combination locks are also acceptable.

(1) MIL-P-17802D (low security), MIL-P-43951 (medium security), or MIL-L-29151 padlocks should be used to add protection to high value, sensitive, and highly pilferable

property. Although there is no MILSPEC standard for security hasps and hinges, other than those available for AA&E storage sites, there is heavy duty security hardware available commercially that would provide added security.

(2) It should be remembered when installing heavy duty hardware that a \$60.00 padlock attached to a 50 cent hasp provides only 50 cents worth of security protection. Additionally, a medium or high security padlock and hasp system realizes its full potential only when it is properly installed on a strong door with appropriate hardware.

d. Employee Education. Each employee must be indoctrinated in local procedures for preventing property losses as well as their responsibility for the care and protection of government property under their control/custody. This indoctrination shall be included in the employee's initial security education briefing upon employment and annually thereafter. Loss prevention topics shall be included in recurring command information and security publications. This shall be closely coordinated with the security manager. (Refer to Chapter 9, Part 1.)

e. Discipline. Administrative personnel actions or action taken pursuant to the Uniform Code of Military Justice are exclusive of actions for recovering government losses through claims litigation. Additionally, civilian authorities may impose criminal sanctions in cases where such action is appropriate after analysis of applicable jurisdiction and other legal considerations.

f. Financial Responsibility. Local procedures for the issue and control of government property will ensure that strict accountability is established for persons responsible for government property which is reported as missing, lost or stolen. Recoupment action should be undertaken against an individual in each case in which the individual's negligence or non-compliance with procedures, instructions or statutes results in a missing, lost or stolen reportable loss of that government property. This recoupment action is independent of and may be taken parallel to, or be exclusive of, any formal disciplinary action, criminal procedures or prosecution arising from the same event.

g. Claims. Individuals accountable for government property must be held legally responsible for negligent loss. The naval activity having missing, lost, stolen, recovered (M-L-S-R) reporting responsibility may generate a claim action to recoup the value of the loss. Specific guidance on local procedures may be obtained from the area Naval Legal Service

16 SEP 1985

Office, other servicing military legal offices, especially the activity Staff Judge Advocate, if one is assigned. The claims collection procedure may result in a civil court action which is independent of any disciplinary action or criminal prosecution which may arise from the same event.

h. Criminal Prosecution. Examination of the facts by command may indicate criminality sufficient to warrant referral to legal authorities for criminal prosecution for violations of law. Criminal prosecution is independent of disciplinary, recoupment or claim action arising from the same incident(s). The security officer is responsible, in conjunction with activity legal counsel, for ensuring that security portions of criminal cases (investigations, evidence, reports, statements, etc.) are prepared properly and in sufficient detail to render them acceptable for prosecution in federal, state, and local courts. The security officer will also monitor the progress of criminal issues and maintain liaison with the activity legal counsel and the Naval Investigative Service to facilitate effective prosecution.

0304. LOSS REPORTING

a. M-L-S-R government property reports will be submitted promptly as required by reference (f). The command security officer shall be the command's focal point for tracking such reports.

b. Effective reporting of losses is basic to the determination of the scope of the loss prevention program which must be developed by the command. When reviewing property losses which are not critical to national security and which do not threaten the civilian population, it is of primary importance to know whether the expenditure of funds on physical security will net a payback in loss reductions. If real losses are extremely low, and involve only non-sensitive, low value, or non-hazardous materials, it may be more cost-effective to absorb such losses. Nevertheless, actual losses must be reported so that an accurate decision can be made by the command. To this end, steps must be taken to ensure that reportable losses and accountable individuals are identified. This can be done by matching property inventories, requests for investigations, inventory adjustments, etc., with loss reports submitted. Historically, many audit and inspection reports have shown that not all required reports are submitted and actual losses have greatly exceeded reported losses. The following definitions are provided to clarify the use of terms used in reference (f) and this instruction.

16 SEP 1985

(1) Missing (M). A missing item is one that is not in its proper location or cannot be readily accounted for. Searches by responsible personnel have been completed without success, the incident has been reported to the activity security officer for action, and the responsible officer (e.g., comptroller, supply officer, etc.) has initiated loss reporting action.

(2) Lost (L). A lost item is one that cannot be found and as a result has been surveyed or otherwise properly removed from accountability, after thorough investigation of the circumstances. If reportable under reference (f), a final report must be submitted on the item.

(3) Stolen (S). A stolen item is one that is not in its proper location or is unaccounted for and evidence indicates actual thefts or other related criminal activity is the reason for its absence.

(4) Recovered (R). A recovered item is a unit of material that is gained by inventory, found, recovered after previously being reported missing, lost or stolen or suspected to be the remainder of a loss due to theft or fraud.

(5) M-L-S-R Reportable Loss/Gain. Any missing, lost, stolen or recovered government property which meets the sensitivity, material category or minimum dollar value criteria contained in reference (f).

(6) Serialized Government Property. Any item of government property which has an individual serial number affixed by the manufacturer.

(7) Unserialized Government Property. Any item of government property which does not have an individual serial number.

(8) Value. The measurement of government property value for M-L-S-R reporting purposes is the current cost of purchasing a new replacement item on the open market (current market value) or the current government price list cost, whichever is greater. Depreciated values will not be used for M-L-S-R reporting or for the purpose of reducing single line item or aggregate item values below M-L-S-R dollar value reporting thresholds.

c. Accountability. In each case of loss, theft or destruction of property that is M-L-S-R reportable in accordance with reference (f), efforts will be made to establish whether the event involved negligence or

16 SEP 1985

non-compliance with established Navy or local procedures/policies. The individual(s) responsible will be determined whenever possible. Persons who are determined to have been negligent or to have failed to comply with established procedures or policies for the handling and control of government property will be identified by rank, rate or grade in the M-L-S-R report as required by reference (f). Section HHH must be properly completed in every initial M-L-S-R report. If accountability (HHH) data (enclosure (2) to reference (f)) is listed as "unknown" at the time of initial report, this information must be provided in pending, final or supplemental reports for the same event.

d. Investigation. All M-L-S-R reportable property incidents involving missing, lost or stolen property must be reported to the nearest field component of the Naval Investigative Service for investigative consideration. Referral, initiation or declination of an investigation by the Naval Investigative Service or the Federal Bureau of Investigation will be fully explained in part (D), Section III of initial M-L-S-R property reports concerning the incident. Enclosure (2) to reference (f) explains the reporting procedures and formatting requirement. M-L-S-R property incidents not investigated by the Naval Investigative Service or the Federal Bureau of Investigation will be carefully reviewed to determine whether the incident requires investigation by the activity or whether the Naval Investigative Service should refer the matter to state and/or local civilian authorities for investigation. If an investigation is initiated, the on-going status of the investigation will be provided during pending or supplemental reports in part (D), Section JJJ (see enclosure (2) to reference (f)). The final M-L-S-R property report will not be issued until all Naval Investigative Service, Federal Bureau of Investigation, police or other known investigative action is completed and the case is closed.

e. Summary Information. Each M-L-S-R property incident will receive special attention and be carefully described. Stock phrases will not be used to explain losses. Repetitive M-L-S-R property incidents involving the same type or class of material is often indicative of a lack of adequate local crime prevention or inventory control procedures; failure to observe existing property controls, loss prevention or inventory control procedures; or a lack of enforcement when procedural violations occur. Causative factors should be identified and prompt corrective action initiated and reported. Specific concerns relative to part (A), section JJJ are as follows:

(1) Care must be taken to explain the detailed circumstances of a loss (required by part (B), Section JJJ of enclosure (2) to reference (f)) in the initial M-L-S-R report or to project the date when an explanation can be expected.

(2) When information is provided concerning the date of the last command inspection or inventory (required by part (B), Section JJJ of enclosure (2) to reference (f)), it shall be clearly indicated whether the date provided is the date of the command inspection or is the date of an inventory.

(3) The narrative comments provided (required by part (C), Section JJJ of enclosure (2) to reference (f)) in initial or subsequent M-L-S-R reports must identify security problems or deficiencies related to the incident. This is especially crucial if the incident appears to be repetitive in nature. Early identification of security problem areas may allow correction prior to an excessive number of costly and avoidable losses.

(4) Reports of disciplinary or administrative action taken (required by part (F), Section JJJ of enclosure (2) to reference (f)) refer to actions taken against persons responsible for the theft, fraud, or similar act regarding government property. This should not be confused with the identification/information and disciplinary or administrative action data (required by parts (B) and (C), Section HHH of enclosure (2) to reference (f)) which pertains to persons alleged, suspected or guilty of negligence or non-compliance with procedures related to missing, lost or stolen government property.

(5) Specific security measures taken as a result of the incident (required by part (G), Section JJJ of enclosure (2) to reference (f)) refer to corrective physical security measures intended to reduce future similar losses. Improvement of physical security within the Department of the Navy is integral to loss prevention. In every report, the reporting activity must provide details of any real or perceived security deficiency and any action taken or planned to correct such deficiencies. If no measures are necessary/taken, this fact should be so stated.

0305. PERIMETER AND AREA PROTECTION AND CONTROL

a. Prior to making decisions to employ security measures, it is important that a thorough risk and threat analysis is performed to determine the degree of physical security required. As reflected in paragraph 0203, in certain cases extensive and costly security measures may be necessary to

16 SEP 1985

protect certain items of security interest. However, in each case, it is the responsibility of the commanding officer of an activity to comply with established security requirements while at the same time working to achieve economy. To achieve this objective, higher echelon security requirements must be clearly understood. Additionally, the relative criticality and vulnerability of the security interest must be evaluated in relationship to a ranking of potential threats, and a given level of security must be calculated to ensure the best possible protection for that threat level at efficient cost. Only after the above preliminary factors are addressed can proper controls be instituted.

b. Installation of perimeter and area protective controls are the first steps in providing actual protection against certain security hazards. These controls are obtained through the use of protective barriers and other security measures. They are intended to define the installation/activity/area boundaries and are used to channel personnel and vehicular access. Security barriers may be natural or structural and are fully addressed in Chapter 6 of this instruction.

0306. AREA DESIGNATION

Different areas and tasks involve different degrees of security interest depending upon their purpose, nature of the work performed within and information and/or materials concerned. For similar reasons, different areas within an activity may have varying degrees of security importance. To address these situations and at the same time facilitate operations and simplify the security system, a careful application of restrictions, controls and protective measures commensurate with these varying degrees or levels of security importance is essential. In some cases, the entire area of an activity may have a uniform degree of security importance requiring only one level of restriction and control. In others, differences in the degree of security importance will require further segregation of certain security interests.

a. Areas will be designated either as restricted areas or non-restricted areas. Restricted areas are established in writing by a commanding officer within his jurisdiction. These areas are established "pursuant to lawful authority and promulgated pursuant to DOD Directive 5200.8, dated 29 July 1980 (enclosed in SECNAVINST 5511.36), and Section 21, Internal Security Act of 1950; Ch. 1024, 64 stat. 1005; 50 U.S.C. 797)." (See reference (g)).

16 SEP 1985

b. Restricted Areas

Three types of restricted areas are established in descending order of importance: exclusion area, limited area and controlled area. All restricted areas shall be posted simply as Restricted Areas (in accordance with sign provisions set forth herein) so as not to single out or draw attention to the importance or criticality of an area. Although restricted areas most frequently pertain to the safeguarding of classified information, there are other valid reasons to establish restricted areas (e.g., mission sensitivity; protection of certain unclassified chemicals, precious metals or precious metal bearing articles; conventional arms, ammunition and explosives; funds; drugs, goods, nuclear material; sensitive or critical assets; and articles having high likelihood of theft) to protect a security interest.

Restricted areas are defined, as follows:

(1) Exclusion Area. An exclusion area is the most secure type of restricted area. It may be within less secure types of restricted areas. It contains a security interest which if lost, stolen, compromised or sabotaged would cause grave damage to the command mission or national security. Access to the exclusion area constitutes, or is considered to constitute, actual access to the security interest or asset.

(2) Limited Area. A limited area is the second most secure type of restricted area. It may be inside of a controlled area, but is never inside of an exclusion area. It contains a security interest which if lost, stolen, compromised, or sabotaged would cause serious damage to the command mission or national security. Uncontrolled or unescorted movement would permit access to the security interest.

(3) Controlled Area. A controlled area is the least secure type of restricted area. It contains a security interest which if lost, stolen, compromised, or sabotaged would cause identifiable damage to the command mission or national security. It may also serve as a buffer zone for exclusion and limited areas, thus providing administrative control, safety, and protection against sabotage, disruption, or potentially threatening acts. Uncontrolled movement may or may not permit access to a security interest or asset.

The following are examples of restricted areas. Except as indicated in paragraph 0306c(4) below, classification as exclusion, limited or controlled area is under the purview of the local commander as dictated by unit mission and the above restricted area definitions.

16 SEP 1985

Aircraft hangers, ramps, hardstands, flight lines and runways.

Aircraft rework areas.

RDT&E Centers.

Piers and wharves.

Arms, ammunition and explosives storage facilities and areas.

Fuel depots and bulk storage tanks, fuel issue points.

Offices, buildings (as designated).

Communications facilities, radio relay facilities, telephone exchange spaces.

Antennas and antenna fields.

Broadcasting facilities.

Warehouses.

Power stations, transformers, master valve and switch spaces.

Water tank areas, water purification facilities, pumping stations.

Open storage areas and yards.

Intrusion detection systems monitoring spaces.

Central storage spaces for keys.

Controlled industrial areas (CIA) at shipyards.

Funds and negotiable instrument storage areas.

Boundary areas next to limited or exclusion areas.

c. Minimum Security Measures Required for Restricted Areas

(1) The following minimum security measures are required for all exclusion areas:

(a) A clearly defined protected perimeter. The perimeter may be a fence, the exterior walls of a building/structure or the outside walls of a space within a

16 SEP 1985

building/structure. If the perimeter is a fence, it must be posted (in accordance with the sign provisions set forth here) at 100 foot (30.48 meters) intervals along the perimeter. Barrier and lighting requirements are set forth in Chapters 6 and 7. If the perimeter is a wall, it will be posted at the point of ingress (also in accordance with the sign provisions set forth here).

(b) A personnel identification and control system, including an access list and entry/departure log. Only visitors need be logged in/out during normal duty hours. After normal duty hours, all personnel accessing the exclusion area will be logged in/out.

(c) Ingress and egress controlled by guards or appropriately trained and cleared personnel within. When secured, access to the area must be controlled by an intrusion detection system or security personnel.

(d) Admission only to persons whose duties require access and who have been granted appropriate authorization. Persons who have not been cleared for access to the security interest contained within an exclusion area may, with appropriate approval, be admitted to such area, but they must be controlled by a cleared activity escort and the security interest protected from compromise.

(e) When secured, checked at least twice per 8 hour shift or, if adequately equipped with an operational IDS, at least once per 8 hour shift. Checks by security force will be for signs of attempted or successful unauthorized entry, and other activity which threatens to degrade the security of the exclusion area.

(2) The following minimum security measures are required for all limited areas:

(a) A clearly defined and protected perimeter. The perimeter may be a fence, the exterior walls of a building/structure or the outside walls of a space within a building/structure. If the perimeter is a fence, it must be posted (in accordance with the sign provisions set forth herein) at 100 foot (30.48 meters) intervals along the perimeter. Barrier and lighting requirements are set forth in Chapters 6 and 7. If the perimeter is a wall, it will be posted at the point of ingress (also in accordance with the sign provisions set forth herein).

(b) A personnel identification and control system. During normal duty hours, use of an access list and

16 SEP 1985

entry/departure log is suggested but not required. After normal duty hours, all personnel accessing the limited area must be logged in/out. (An electronic control system with the capability of recording ingress/egress may be used to accomplish this).

(c) Ingress and egress controlled by guards, receptionists or other appropriately trained and cleared personnel within.

(d) Admission only to persons whose duties require access and who have been granted appropriate authorization. Persons who have not been cleared for access to the security interest contained within a limited area may, with appropriate approval, be admitted to such area, but they must be controlled by a cleared activity escort, and the security interest protected from compromise or other degradation.

(e) When secured, checked at least twice per 8 hour shift or, if adequately equipped with an operational IDS, at least once per 8 hour shift. Checks by security force will be for signs of attempted or successful unauthorized entry, and other activity which threatens to degrade the security of the limited area.

(3) The following minimum security measures are required for all controlled areas:

(a) A clearly defined protected perimeter. The perimeter may be a fence, the exterior walls of a building/structure or the outside walls of a space within a building/structure. If the perimeter is a fence, it must be posted (in accordance with the sign provisions set forth herein) at 100 foot (30.48 meters) intervals along the perimeter. Barrier and lighting requirements are set forth in Chapters 6 and 7. If the perimeter is a wall, it will be posted at the point of ingress (also in accordance with the sign provisions set forth herein).

(b) A personnel identification and control system.

(c) Ingress and egress controlled by guards, receptionists or other appropriately trained and cleared personnel within.

(d) Controlled admission of individuals (military, civil service, contractors, official visitors) who require access for reasons of employment/official business, individuals who render a service (vendors, delivery people), dependents, retired military and unofficial visitors (guests of residents, visiting softball team, etc.). Individuals without adequate identification as determined by the local commander must be logged in/out.

16 SEP 1985

(4) Certain facilities and assets have been identified as especially critical and essential to the overall mission of the Navy and the national security. These have been identified in Appendix IX. Restricted area designations have been individually assigned in addition to specific physical security requirements to provide optimum protection for these facilities/assets.

(5) All instructions designating restricted areas shall include procedures for conducting inspections of persons and vehicles entering and leaving such areas. The purpose is to detect/prevent the introduction of prohibited items (firearms, explosives, drugs, etc.) and to detect/prevent the unauthorized removal of government property/material. To be effective, administrative inspection operations should be conducted on a random basis at least daily. As a minimum, however, they are required weekly. Procedures will be approved by the cognizant Staff Judge Advocate or Navy Legal Service Office.

d. Non-Restricted Areas

(1) A non-restricted area is an area which is under the jurisdiction of an activity, but to which access is either minimally controlled or uncontrolled. Such an area may be fenced, but may be open to the uncontrolled movement of the general public at various times. An example of a non-restricted area is a visitor or employee parking lot open and unattended by guards during business hours. After business hours it may be closed, patrolled and converted to a restricted area. Another example is a personnel office to which the general public is permitted access during business hours without being required to check in or register with the security office. A non-restricted area could be an area enclosed by a fence or other barrier, to which access would be minimally controlled by a check point which would only ensure that the visit or access was for official business or other authorized purpose. In such cases further security authorization would not be required for access, e.g., a security clearance. A housing area, exterior to base would normally be designated as a non-restricted area. Non-restricted areas will not be located inside restricted areas.

(2) Many naval activities and installations have areas containing a number of facilities to which members of the armed forces and their dependents, as well as civilian employees and their families, are permitted access by displaying vehicle decals or by presenting appropriate identification cards (not issued on the basis of security

16 SEP 1985

clearance or similar screening, but by virtue of employment or status). These facilities include exchanges, commissaries, administrative offices, dispensaries, clubs, recreational facilities, etc. Areas containing these facilities on activities and installations normally will be designated as non-restricted areas. (However, it is recognized that these facilities themselves may have internal spaces which will of necessity be designated as restricted areas.)

0307. SIGNS AND POSTING OF BOUNDARIES

a. Restricted areas (including buildings) will be posted at all external points of ingress with signs approximately three feet (0.91 meters) by three feet in size with proportionate lettering. Signs will read as follows:

WARNING

RESTRICTED AREA - KEEP OUT
AUTHORIZED PERSONNEL ONLY

AUTHORIZED ENTRY INTO THIS RESTRICTED AREA CONSTITUTES
CONSENT TO SEARCH OF PERSONNEL AND THE PROPERTY UNDER
THEIR CONTROL.

INTERNAL SECURITY ACT OF 1950 SECTION 21; 50 U.S.C. 797 (1976).

(1) Internal points of ingress into designated exclusion or limited areas within a controlled area building may be designated with the appropriate warning signs, i.e., "Warning - Exclusion (or Limited) Area - Keep Out - Authorized Personnel Only".

(2) Internal points of ingress into designated controlled, limited, or exclusion areas within a non-restricted area building may be designated with the appropriate warning signs as illustrated in 0307b below.

b. Perimeter barriers of all restricted areas will be posted with signs measuring approximately twelve inches (0.3 meters) by eighteen inches (0.45 meters) in size with proportionate lettering. Signs will read:

16 SEP 1985

WARNING
RESTRICTED AREA
KEEP OUT

Authorized
Personnel Only

c. Non-restricted areas will be posted at all points of ingress with signs approximately three feet (0.91 meters) by three feet in size with proportionate lettering. Signs will read as follows:

WARNING
U.S. NAVY PROPERTY
AUTHORIZED PERSONNEL ONLY

AUTHORIZED ENTRY ONTO THIS INSTALLATION CONSTITUTES CONSENT TO SEARCH OF PERSONNEL AND THE PROPERTY UNDER THEIR CONTROL.

INTERNAL SECURITY ACT OF 1950 SECTION 21; 50 U.S.C. 797 (1976)

d. Perimeters of all non-restricted areas will be posted with signs measuring approximately eleven inches (279 mm) by twelve inches (0.3 meters) in size with proportionate lettering. Signs will read:

U. S. GOVERNMENT PROPERTY
NO TRESPASSING

e. Where a language other than English is prevalent, restricted and non-restricted area warning notices will be posted in both English and the local language.

f. The interval between signs posted along non-restricted area perimeters will be 200 feet (61 meters).

g. All barrier signs should be placed so as not to obscure the necessary lines of vision for security force personnel.

h. Color Code. All signs shall be color coded to provide legibility from a distance of at least 50 feet (15.2 meters) during daylight under normal conditions. The following codes are recommended for installation/activity and restricted area perimeter signs:

(1) All words except "WARNING" should be black.

(2) The word "WARNING" should be red.

(3) All wording should be on red, white, and/or blue backgrounds as appropriate to obtain maximum color contrast.

16 SEP 1985

i. Standard Non-Restricted Area Signs. Plastic non-restricted area perimeter warning signs measuring approximately 10 1/4" (26.0 cm) x 11 1/2" (29.2 cm) are available through supply channels under NSN #9905-00-559-2971. These signs are shaped in the form of a shield, have a combination red, white, and blue background and bear the words "U.S. PROPERTY - NO TRESPASSING". These signs are approved for use.

0308. KEY SECURITY AND LOCK CONTROL

Each naval activity must establish a strict key and lock control program managed and supervised by the activity security officer. Included within this program are all keys, locks, padlocks and locking devices used to protect or secure restricted areas and activity perimeters, security facilities, critical assets, classified material and sensitive materials and supplies. Not included in this program are keys, locks and padlocks for convenience, privacy, administrative or personal use.

a. Key Control Officer. The key control officer will be designated in writing by the commanding officer and be directly responsible for all security-related key and lock control functions at the activity. Normally, the key control officer is subordinate to the security officer. At those activities where the security key and lock program is too small to warrant a subordinate designation, the security officer assumes this function. The key control officer will conduct an annual inventory of all issued keys at the activity and will maintain appropriate logs and records.

b. Key Custodian. The head of each major functional area (i.e., department, directorate, etc.) within an activity will designate in writing a key custodian who will be responsible to the key control officer for all keys controlled by that functional area. Each custodian may have sub-custodians as operationally necessary to accomplish the mission. Each custodian will inventory keys issued to custodial and sub-custodial key log accounts at least monthly.

c. Central Key Room. Duplicate keys, key blanks, padlocks (key and combination type) and key making equipment will be stored in a central key room. Access must be controlled and the space must be secured when not in use. Duplicate keys will be provided protection equivalent to the asset/area that original keys are used to secure.

(1) At those activities where the security key and lock program is too small to warrant a central key room, security containers with a three-position combination lock may be used to provide protection of duplicate keys, blanks and associated equipment.

d. Rotation and Maintenance. Security locks, padlocks and/or lock cores shall be rotated from one location to another within the same level areas of protection (i.e., limited area locks, cores stay within limited areas, etc.) at least annually or more frequently if deemed appropriate. Rotation is accomplished to guard against the use of illegally duplicated keys and to afford the opportunity for regular maintenance to avoid lockouts or security violations due to malfunction because of dirt, corrosion and wear.

e. Criteria for Issuing Keys. Keys for security locks and padlocks must be issued only to those persons with a need approved by the activity security officer. Convenience or status is not sufficient criteria for issue of a security key. Also, certain categories of security assets have specific rules concerning the issue and control of keys affording access to them. The activity security officer is responsible for developing and enforcing rules for key issue as part of his/her access control function.

f. Key Control. The central keyroom and each key custodian and sub-custodian must institute a system showing keys on hand, keys issued, to whom, date/time the keys were issued and returned, and the signatures of persons drawing or returning a security key. Continuous accountability of keys is required at all times.

g. Padlock In-Use Security. When the door, gate or other equipment which the padlock is intended to secure is open or operable, the padlock will be locked into the staple, fence fabric, or other nearby securing point to preclude the switching of the padlock to facilitate surreptitious entry.

h. Lock Control Seals. Inactive or infrequently used gates must be locked and have seals affixed. The approved seal is the car ball end seal, Military Specification MIL-S-23769C. Security personnel should be instructed that lack of freeplay (approximately one-eighth inch) indicates the possibility of tampering and a follow-up examination of the seal should be conducted. Seals must be serialized and should be stored in the central keyroom. The activity security officer will control placement of entrance seals and account for seal numbers on-hand, issued and used.

i. Procurement of Locks and Padlocks. All locks and padlocks used for low, medium and high security applications will meet the minimum military specifications for that level of security use. All security lock and padlock procurement at an activity must be approved by the activity security officer.

16 SEP 1985

j. Lockouts. All lockouts involving restricted areas/buildings must be investigated by security force personnel to determine if the failure of the locking device occurred because of a product failure or as a result of attempted or actual illegal penetration.

0309. STORAGE CONTAINERS, VAULTS AND STRONGROOMS

Security containers, vaults and strongrooms will conform to the specifications contained in reference (a).

0310. SECURITY SURVEYS AND INSPECTIONS

Each naval activity and installation will establish a program to assess the degree of local compliance with the security standards, requirements and policies contained in or referenced by this instruction on an annual basis. The physical security survey checklist contained in Appendix VIII should be used. Command inspections or special purpose (physical security inspection/physical security audit/physical security review) examinations of an activity security program will be conducted by an immediate superior in command at least triennially and will include the practical exercise of physical security, loss prevention and crises management plans to evaluate the overall adequacy of the security force and the activity's ability to protect against penetration of its barriers and unauthorized entry, protect vital property and deal with terrorist situations.

0311. SECURITY CHECKS

Each naval activity must establish a system for the daily after-hours (also weekends) checking of security areas, facilities, containers, and barrier or building ingress/egress points to detect any deficiencies or violations of security standards. Security deficiencies or violations found during after-hour checks must be reported to the activity security officer, the department involved and the commanding officer. These incidents will also be reported to activity departments or other local elements having security responsibilities within specific security programs affected by the incident. Each deficiency or violation must be followed up by the activity security officer and a record kept of all actions taken (structural, security, disciplinary, administrative, etc.) by the responsible department or elements involved to resolve the present deficiency or violations and to prevent recurrence. All security deficiencies, violations, breaches of security rules and regulations and criminal incidents discovered and handled by the security force will be recorded on OPNAV Form 5527/1 (Incident/Complaint Report).

16 SEP 1985

0312. PARKING OF PRIVATELY OWNED VEHICLES (POV)

a. As a general rule, employees will not be permitted to park adjacent to work spaces. Privately owned vehicles will not be parked in exclusion and limited areas or within 30 feet (9 meters) of doorways leading into or from building primarily used for the manufacture, repair, rework, storage, handling, packaging or shipping of government materials and supplies at naval activities. Management of the parking assignment function is not a function of physical security and the security officer's duties do not include parking assignments. The activity security officer however, being responsible for access and movement controls for all activity restricted areas and for the activity loss prevention program, should be in the approval chain for the following:

(1) Requests for approval of any parking lot in a controlled area or within 30 feet (9 meters) of doorways leading into buildings described above.

(2) Establishment of policy and criteria for parking assignments in controlled areas or within 30 feet (9 meters) of doorways leading into buildings described above.

(3) Approval of any proposed individual exception to parking policy or criteria.

b. At activities where parking is allowed inside controlled areas, parking areas will be located away from exclusion/limited areas and separately fenced in such a manner that occupants of vehicles must pass through a guarded pedestrian gate before entering the actual restricted area facility. Vehicle parking is prohibited within 15 feet (4.5 meters) of any building to minimize danger in the event of fire or explosion.

0313. TRAFFIC CONTROL

The security officer at host installations must establish an effective traffic control program in accordance with references (h), (i), (j) and (k). Traffic enforcement and accident investigations where proprietary or concurrent jurisdiction is prevalent will fully comply with local, state and Federal laws and requirements. Where exclusive jurisdiction is prevalent, traffic management should be handled under the provisions of reference (k) using the Assimilative Crimes Act.

16 SEP 1985

0314. SECURITY OF SELECTED, SENSITIVE INVENTORY ITEMS -
DRUGS, DRUG ABUSE ITEMS AND PRECIOUS METALS

The following definitions describe sensitive items:

- a. Selected Sensitive Inventory Items. Those items security coded "Q" or "R" in the Defense Integrated Data System (DIDS) that are controlled substances, drug abuse items or precious metals.
- b. Code "Q" Items. A drug or other controlled substance designated as a Schedule II, IV or V item, in accordance with 21 Code of Federal Regulations, Part 1308, an extract of which is contained in Appendix X.
- c. Code "R" Items. A drug or other controlled substance designated as a Schedule I or II item in accordance with 21 Code of Federal Regulations, Part 1308 as well as precious metals (defined below).
- d. Precious Metals. Refined silver, gold, platinum, palladium, iridium, rhodium, osmium, and ruthenium in bar, ingot, granulation, sponge or wire form.

0315. SECURITY REQUIREMENTS FOR "R" CODED ITEMS AT BASE AND
INSTALLATION SUPPLY LEVEL OR HIGHER

- a. Stored in Class "A" vaults (as defined in reference (a)) or 750 pound or heavier General Services Administration (GSA) approved security containers. Smaller GSA approved security containers are authorized but must be securely anchored to the floor or wall. All security containers will be secured with built-in Group One combination locks.
- b. If stored within a vault, the vault door must be protected with a balanced magnetic door switch and any vents/openings protected in accordance with Chapter 8.
- c. If stored within security containers, they must be protected with intrusion detection equipment as described in Chapter 8.
- d. Intrusion detection equipment must be connected to a central monitoring station manned 24 hours per day with a capability to provide an armed response to an alarm signal within five minutes.

0316. SECURITY REQUIREMENTS FOR "O" CODED ITEMS AT BASE AND
INSTALLATION SUPPLY LEVEL OR HIGHER

- a. Stored in Class "A" vaults or security containers as described in paragraph 0315.

16 SEP 1985

b. An alternative is to store these items in an exclusion area as described in paragraph 0306c(1). This area must also be equipped with an approved intrusion detection system (IDS) connected to a central monitoring station manned by armed guards capable of responding to an alarm within five minutes.

0317. SECURITY REQUIREMENTS FOR "R" AND "Q" CODED ITEMS BELOW BASE AND INSTALLATION LEVEL (i.e., small unit/individual supplies)

a. Stored as described in paragraphs 0315 and 0316.

b. As an alternative, small stocks may be stored in a 750 pound or heavier GSA approved security container. Smaller GSA approved security containers are authorized but must be securely anchored to the floor or wall. Security containers must be located within a continuously manned space or must be checked hourly by a security force member.

0318. SECURITY OF FUNDS - DISBURSING OFFICE

The physical security requirement for funds under control of a disbursing officer or stored within a disbursing office are contained in the NAVCOMPT Manual. The appropriate paragraph is included as Appendix XI.

0319. ELECTRIC TYPEWRITERS, CALCULATORS, ADDING MACHINES, ETC.

Electric typewriters, calculators, adding machines, and similar items of office equipment, will be secured to preclude pilferage. When an office space is vacant during non-duty hours, doors will be secured and access controlled or these items of equipment will be secured in security containers, or storage cabinets. As an alternative, electric typewriters and similar items may be secured to desks with commercially available anchor pads.

0320. VIDEO RECORDERS, TELEVISIONS, FILM PROJECTORS, RADIO RECEIVERS, ETC.

Video-recorders, televisions, film projectors, radio receivers, and similar items used for mission related audio visual purposes will be stored within spaces to which access is controlled during normal duty hours. After normal duty hours, these items will be secured in a locked room and key control procedures instituted.

OPNAVINST 5530.14A

16 SEP 1985

0321. TELEVISIONS (WITHIN LOUNGES, QUARTERS, ETC.)

Government owned televisions within clubs, lounges, transient and permanent personnel housing will be secured to prevent theft. A recommended method is to secure the item in place with a commercially available anchor pad.

CHAPTER 4

THE SECURITY FORCE

0400. GENERAL

The security force constitutes one of the most important elements of an activity's physical security program. It provides the enforcement implementation medium in the physical security effort. The security force consists of designated persons specifically organized, trained, and equipped to provide the physical security for the command. Properly used, it is one of the commander's most effective and useful tools in a comprehensive, integrated physical security program. Security forces at naval activities may be composed of:

- a. DOD civilian security police.
- b. DOD civilian security guards.
- c. General services administration (GSA) guards.
- d. Contract guards (commercial security services).
- e. Military force (Navy and Marine Corps personnel).
- f. Combinations of the above.

NOTE: In overseas locations certain naval activities are also protected by foreign nationals. In such cases rules and policies governing these guards as part of the security force will be determined locally in accordance with applicable agreements.

0401. MARINE CORPS SECURITY FORCE (MCSF)

Guidance for the appropriate employment of MCSF components is set forth in reference (1). The primary mission of MCSF components is to provide physical security for those portions of naval activities or vessels that require the unique capabilities of an armed, combat-trained marine.

0402. FUNCTIONS OF THE SECURITY FORCE

Regardless of the type of security force employed, their functions fall into three general categories:

- a. Protect life, property and the rights of individual citizens.

16 SEP 1985

b. Prevent/deter theft and other losses, i.e., fire, damage, accident, trespass, sabotage, espionage, etc.

c. Enforce security, rules, regulations and policies.

0403. THE SECURITY OFFICER AND THE SECURITY FORCE

As discussed in Chapter 1, the security officer heads the physical security organization of a naval activity or installation, and in this capacity, plans, implements and supervises the physical security program. Specific duties, in addition to those listed in Chapter 1, will include, but are not limited to:

a. Supervising, organizing and training the security force.

b. Managing the activity's law enforcement, security force and Master-at-Arms functions.

c. Identifying the number of posts, patrols, and strengths of the police/guard and crisis response force (CRF) (hereafter referred to collectively as the "security force") sufficient to protect, react to and confront situations and circumstances which threaten personnel and property.

d. Identifying post orders, standard operating procedures, and training for the security force, which includes jurisdiction, use of force, apprehension and temporary detention of intruders and violators, and other appropriate topics.

e. Developing written physical security orders and/or directives to cover all phases of security operations.

0404. ASSIGNMENT OF SECURITY OFFICERS

The quality of direction provided to the security force by the security officer will have major impact on the activity's security program. The letter of designation will include a statement requiring the security officer to be knowledgeable of the duties specified in paragraph 0403. The importance of the billet dictates that the security officer possess:

a. Appropriate grade/rank.

b. Broad military/civilian security experience.

c. Mature judgement.

16 SEP 1985

The commanding officer of the Marine barracks or detachment may only be assigned as the activity security officer upon the approval of the Chief of Naval Operations (OP-09N) with the concurrence of the Commandant of the Marine Corps.

0405. SIZE OF SECURITY FORCE

The size of the security force is dependent upon many factors. Examples are:

- a. Size and location of the activity.
- b. Mission of the activity.
- c. Number, type and size of security areas.
- d. Use of alternate security support measures and effectiveness of mechanical or electronic security measures employed.
- e. Security force support provided by other agencies.
- f. Total daily population of the installation and its composition.

0406. LEGAL AUTHORITY

Appendices V and VI contain information pertaining to legal authority relevant to the security of naval installations and authority of commanding officers to act in furtherance thereof.

0407. SECURITY FORCE ORDERS

Every activity will publish and maintain security force orders pertaining to each post. The concept of security force orders is as follows:

- a. Security force orders are the written and approved authority for members of the force to execute and enforce such orders and regulations as the commanding officer of an activity may prescribe.
- b. All security force orders will specify the limits of the post, specific duties, the hours the post is to be manned as well as the uniform, arms and equipment prescribed for members of the security force. Additionally, all orders will contain guidance on the use of force as outlined in reference (n).

16 SEP 1985

c. All security force orders will be brief, concise, specific and current. They should be prepared in the affirmative and written in clear and simple language. Security force orders will be under constant review for currency and will be updated as required. The security officer will conduct a total detailed review at least semi-annually.

d. Security force orders for military and civilian guards/police will be approved and signed by the Security Officer with copies to the Commanding Officer.

0408. SECURITY CLEARANCE FOR SECURITY FORCE PERSONNEL

A security clearance is an administrative determination by competent authority that an individual's reliability, honesty, loyalty, judgement, and trustworthiness are such that allowing access to classified information is clearly consistent with the interests of national security. The controlling factor in determining the level of clearance which is required for any given position is the level of classified information or restricted area to which the incumbent needs.

0409. CIVILIAN SECURITY FORCE

The two categories of civilians performing security force duties are General Schedule civil service employees and contract security force personnel furnished by private agencies under contract to the using activity.

a. Selection of Civil Service Security Force Personnel. Care in the initial selection of security force personnel and in the elimination of the marginal performer during early training is important. Turnover in the security force is undesirable for the following reasons:

(1) Release of personnel trained in sensitive operations creates a possible source of information for persons seeking to discover vulnerable points of a security system.

(2) There is a high cost factor in training replacements.

(3) Frequent turnover breaks continuity of procedural familiarity and experience, which results in reduced readiness and less effective protection.

b. General Requirements. Minimum civil service qualifications of security force personnel are specified in civil service qualification standards and must be adhered to in all classification and selection matters. In general, security force personnel should be physically agile, mentally alert and

16 SEP 1985

possess good judgement. Positions will be established in a particular job series on the basis of duties actually performed (i.e., a position with more than 50 percent police duties will be classified in the Police Series (GS-083)).

c. Composite Security Force. When Naval activities qualify for MCSF protection, there is nothing to preclude the use of a composite security force of civilian and military personnel as long as each element of the security force is assigned duties in accordance with directed requirements. Marines in the security force will be assigned duties in accordance with guidelines set forth in reference (1). When a composite force is in place, DOD police and Navy MAA assets should be incorporated into one supervisory echelon.

d. Integration of Police and Fire Protection. Activities will not consolidate or integrate police or guard forces with fire protection forces without the approval of the Chief of Naval Operations (OP-09N); but the security officer may supervise fire protection forces as a separate function.

e. Personal Supervision. Where a security force is in place, close personal supervision is a necessary element for a successful security program. Personal supervision will include the following:

(1) Inspecting security force personnel by a supervisor prior to posting. At this time, special instructions or orders are provided.

(2) Inspecting each security post or other security activity by security supervisors at least twice per shift to insure that personnel and systems are functioning properly.

f. Indirect Supervision. Various means may be used to facilitate/supplement personal supervision of security forces. Two such means include:

(1) Recorded Tour Systems. Under these systems, security forces record their patrols or presence at designated places throughout the installation by use of portable watch-clocks, central watch-clock stations or similar devices. These systems are an effective means of ensuring that certain points are regularly patrolled.

(2) Call-In Boxes. Telephone boxes can be located at points throughout large installations. Security forces can use these to call in and report or receive instructions.

0410. DETERMINATION OF SECURITY FORCE STRENGTH

The number of positions in the security force are normally based on the number of twenty-four hour posts to be manned. The total number of personnel assigned to the security force for a given number of posts depends on the type of force, for example:

a. A post manned by enlisted Marines normally requires six Marines per post.

b. A post manned by enlisted naval personnel normally requires five personnel per post.

c. A post manned by civil service or contract security personnel varies in the requirement for the number of persons per post. Overhead, differences in missions, supporting personnel and special training account for the differences in manning requirements. The formula for calculating general requirements is shown in paragraph 0414.

0411. DETERMINATION OF POSTS

Since no two activities will present the same degree of risk or contain identical situations, it is impractical to set fixed rules to apply to all activities. Commanding officers must perform an analysis of their command to determine the number and type of posts required to provide optimum and cost-effective protection. Consideration should be given to employing alternate security measures such as electronic intrusion detection systems, closed circuit television, securing nonessential gates, etc.

0412. TYPES OF POSTS

Posts will normally be of three basic types:

a. Fixed. Where security personnel normally remain at one point or within a specific area, i.e., gates, towers.

b. Mobile. These posts may also be referred to as roving patrols. They are used for perimeter surveillance, area patrols, etc. Security forces may be on foot, in vehicles, boats, or on bicycles/motorcycles.

c. Administrative. These include the security or police chief and other supervisory personnel; identification and pass clerks; dispatchers; alarm system monitoring personnel; locksmiths; law enforcement and security training specialists; physical security specialists; traffic and criminal investigators; clerks and stenographers, etc.

0413. POST REQUIREMENTS AND CONSIDERATIONS

a. Gates. Gates will be limited to the minimum number required to permit the expeditious flow of traffic in and out of the activity. Except where justified by consistently heavy traffic throughout the day or by other security considerations, one sentry per gate will normally suffice. Rush hour augmented post manning must be included in post calculations. Bear in mind that personnel obtained temporarily for fixed posts from mobile posts reduces emergency response capability to alarms, accidents and traffic problems. Full-time use of a guard at a railroad gate or a construction gate when nothing more than intermittent use is made of the gate may not be justified unless the sentry has collateral duties.

b. Perimeter. The justification for perimeter posts is in direct proportion to the necessity for preventing unauthorized entry. Activity "A" may be of such nature as to require that inviolability must be maintained at all costs. Perimeter protection here would call for a combination of approved fencing, protective lighting, and intrusion alarms, all supported by numerous fixed posts and with mobile patrols operating in relatively small areas. On the other hand, Activity "B" meets security requirements by using nothing more than a fixed or mobile post. The perimeter protection requirements for most activities will be found somewhere between these extremes and are discussed in paragraph 0306.

c. Area Posts. As with perimeter protection, guarding of areas must be commensurate with the importance of the area and the threat. See Chapter 3 for restricted and non-restricted areas.

d. Motorized Patrols. Except under special circumstances, one person vehicles are normally adequate for vehicular patrols.

e. Visitor Escorts. It is not appropriate to establish full-time security posts for visitor escort purposes. The "person to be seen" or his representative will escort to and from the gate. Similarly, in the case of off-station trucks, the department to which shipments are consigned will furnish necessary escorts, unless specific directives concerning the type or sensitivity of the shipment require an armed security escort.

f. Funds Escorts. Armed security force personnel must be provided for official couriers carrying funds in the amount of \$1,000 or more from one installation activity to another on or off base. Escorts for off base funds movement must comply

with applicable state and local laws concerning weapons and emergency vehicles. Coordination with local NIS and Navy JAG office is recommended. If funds escort requirements can be anticipated on a frequent or recurring basis, use of commercial armored car service will satisfy this requirement.

0414. FORMULA FOR ESTIMATING CIVILIAN SECURITY FORCE STRENGTH REQUIREMENTS

a. After the desired number of actual security posts has been determined, the approximate number of security personnel needed can be calculated as follows:

EXAMPLE

One post (abstract) requires 168 man-hours per week (1 man, 7 days, 24 hours). Compute the total number of man-hours per week for all actual posts and divide by 168. This gives the number of abstract posts. Ascertain the average number of days of annual leave and sick leave that will probably be required. From the following table, find the "number of guards per posts required" appropriate to the average leave anticipated. Multiply this figure by the number of posts required.

If average number of days off for annual and sick leave anticipated per individual is:	Number of personnel per post required (40-hour week)
---	--

0 (basic).....	4.2
20.....	4.55
25.....	4.65
30.....	4.75
35.....	4.85
40.....	4.96

EXAMPLE

POST #1	1 individual, 24 hours, 7 days = 168 hours
Gate	1 individual, 10 hours, 5 days = 50 hours
Patrol	1 individual, 2 hours, 5 days = 10 hours
POST #2	1 individual, 24 hours, 7 days = 168 hours

TOTAL hours = 396

POST #3 2 personnel, 16 hours, 7 days = 224 hours

1 individual, 8 hours, 2 days = 16 hours

TOTAL hours = 240

Grand total is 636 man-hours per week, which divided by 168, gives 3.78 posts. Average leave anticipated is 30 days per individual. The table shows that in this case 4.75 personnel per post are required for each of the 3.78 posts or a total of 17.95 security force personnel.

b. Supervisory personnel may be included in the post calculations or separately added.

c. It is recognized that it may be difficult to determine the average number of days annual and sick leave. However, by using the experience of previous years, a reasonably accurate figure should be obtained.

d. It must also be pointed out that in some cases, particularly those involving security forces of small size, scheduling of work hours to give post coverage as it is needed may not be entirely practicable if the security force requirements are based on a strict minimum application of the above formula.

e. The formula indicated does not reflect man-hours required for initial, annual and specialized training, special details and miscellaneous assignments. If special assignments are valid security responsibilities and the man-hour requirements are fairly consistent and can be gauged on the basis of "averages" indicated by past experience, appropriate adjustment of security forces can be made with little difficulty. However, if such requirements are intermittent or generally of limited duration, consideration should be given to elimination of special details or miscellaneous assignments which are not valid security functions, and instead consider the use of overtime, temporary curtailment or doubling up of posts to accomplish valid assignments and details.

f. In the matter of training, a security force organization with a high turnover rate and inexperienced personnel will undoubtedly require more training than a force that has been in existence for some time with little turnover in personnel. However, even when considerable initial and annual refresher training is required over a period of time, the total man-hours so expended will not normally justify more than one or two training positions for the average security force.

0415. SUPERVISORY STRENGTH

Each shift of security force personnel will have a security supervisor. The ratio of security supervisors to security personnel varies with the overall size of the security force, the extent of its operations and the type and frequency of supervision desired.

0416. MILITARY ARMED GUARDS

Military armed guards for the protection of classified or sensitive shipments transported within the continental United States will be provided by the naval command originating the shipment. Shipments of arms, ammunition and explosives are addressed in reference (e). When appropriate, Armed Forces Courier Service may be utilized for classified material as stated in reference (a).

0417. AUGMENTATION OF SECURITY FORCE FOR EMERGENCIES

Plans must be prepared as a part of the Crisis Management portion of the Physical Security Plan for the use of security force personnel to provide additional security, as required, during emergencies and for augmentation by other additional personnel and equipment. These plans may also provide for the essential training of augmentation personnel and rapid identification and acquisition of emergency equipment and supplies.

0418. CRISIS RESPONSE FORCE

a. General. Each naval installation shall organize, equip and train its own crisis response force to prevent disruption by onboard civil disturbances, repel or contain overt attack by criminal/terrorist elements and to rapidly restore the essential activities which may have been disrupted by civil disturbance, overt attack, natural disaster or other crisis. The CRF will consist of on-board personnel, including civil service personnel that may be utilized as the CRF, augmented and supported by other personnel as considered necessary. Other civilian employees may be utilized as crisis management support/staff elements of the CRF for such functions as medical assistance, firefighting, construction, casualty evacuation, communications, etc.

b. Organization. The CRF should consist of security, control and administrative elements. The security elements should be homogeneously organized, i.e., civilian security force personnel, military security personnel, and other military

active duty personnel as considered necessary. Without SECNAV approval, Marine Corps Security Force personnel can provide only limited assistance as provided in reference (1). Control and administrative elements are those elements which are necessary for command and support of the security elements.

c. Size and Composition. The size and composition of the CRF will depend largely on the size of the installation or activity, geographical location, criticality of assets, vulnerability and accessibility, as determined by the commanding officer. The CRF should provide for the effective utilization of available assets consistent with the continuation of all essential functions during the crisis situation.

d. Command and Control

(1) The commander of major installations may organize the CRF using elements of subordinate and tenant activities as considered necessary. Tenant activities will be responsive to the major installation commanders in the organization, use and training of the CRF.

(2) If an installation CRF is to be employed in conjunction with ships Self Defense Forces, all units will be responsive to the overall direction of the installation CRF Officer.

e. Training

(1) Because elements of the CRF will be involved in the containment of civil disturbances, it is essential that members be trained in the appropriate use of force, legal constraints on use of force and be thoroughly competent in the use of assigned weapons and equipment.

(2) A CRF will receive the following minimum training:

(a) All personnel of the CRF under arms will be qualified with the weapon with which they are armed and will receive indoctrination in the use of force.

(b) Security elements of the CRF will receive training in crisis containment/control and combat operations.

(c) All personnel of the CRF support and administrative elements will receive training in the mission they are to perform.

(d) CRF training schedules are to be established and monitored by the Security Officer.

16 SEP 1985

(e) Marine Corps elements of the CRF will receive training in accordance with Marine Corps directives.

(f) All elements of the CRF will participate in a practical exercise of the CRF at least twice annually. Exercises should be realistically tailored to prepare the CRF for terrorists or other incidents that may occur within their area of responsibility.

f. Small Arms/Weapons/Equipment

(1) All personnel of the CRF will be provided with the small arms/weapons and equipment necessary to perform the missions described above. Establishment of and changes to small arms/weapons allowances will be requested by the individual activity in accordance with NAVMATINST 8300.1A, Small Arms and Weapons Management Program.

(2) Initial issue and replacement of the approved small arms/weapons will be provided at no cost to the requesting activity. All other security equipment is to be procured using installation funds.

(3) The equipment required for Marine Corps Security Forces (MCSF) will be provided by the Marine Corps in accordance with the NAVCOMPT Manual, paragraph 075125.

0419. POLICE FORCES. Tenant activities shall not establish an independent law enforcement (police) function if the host command has a police department tasked with providing law enforcement services throughout the installation. This does not restrict tenant commands from establishing an internal guard force for physical security/loss prevention purposes.

16 SEP 1985

CHAPTER 5

PERSONNEL AND VEHICLE MOVEMENT CONTROL0500. GENERAL

A system of personnel and vehicle movement control is a basic security measure required at naval installations and activities. Positive identification provides a means for visually establishing authorization for personnel movement and actions within the boundaries of a naval activity. Monitoring movement by security and operating personnel is facilitated by requiring the display or presentation of identification. The degree of movement must be in keeping with the sensitivity/classification, value, or operational importance of the area. Procedures must be simple. Visitor control relative to classified information will be in compliance with reference (a).

0501. PURPOSE

The purpose of establishing a personnel and vehicle control system is to provide a visible means to identify and track personnel and vehicles authorized access to an area and deny access to those not authorized.

0502. PERSONNEL IDENTIFICATION AND MOVEMENT CONTROL SYSTEM

The following systems may be used separately or collectively to provide the degree of security desired:

a. Military and Dependent Identification Cards. These cards may be used as a means of identification of personnel authorized access to areas which do not have security implications. This system provides the least secure means of determining authorization for access.

b. U. S. Government Identification Card. Civil service employees may be issued U. S. Government Identification Cards (Optional Form 55), as set forth in the Federal Personnel Manual 295-17, sub-chapter 8, Inst. 199 of 13 September 1973. Even though this form is authorized and recognized as official identification, it will not be used, by itself, to establish authority for entry into areas which have security implications. The form may be used as a media for automated processing of administrative requirements such as timekeeping, tool control, medical benefits, etc.

c. Personal Recognition Systems. Personal recognition is the most positive method of identification for small numbers of personnel and should be utilized wherever feasible.

d. Pass and Badge System. Where the area is large or where the number of personnel exceeds that which can be personally recognized by the guard or persons charged with security responsibility of the area, a pass and badge identification system will be used. Security badges will be used primarily for access controls. Paragraph 0504 establishes minimum standards for identification badges and passes to be used at naval activities.

e. Access List System. Admission of personnel to areas as defined in paragraph 0306 will be granted only to those persons who are positively identified. For exclusion areas, names of persons authorized access must appear on a properly authenticated access list. Lists may be used for access to limited and controlled areas at the discretion of the commanding officer. These lists will be maintained and kept current and under stringent control of an individual who is formally designated by the commanding officer. Admission of persons other than those on the authorized access list will be approved by the commanding officer or designated representative. Access lists will be carefully controlled and not displayed to public view.

f. Exchange Pass System. The exchange pass system is an identification system which may be employed in highly sensitive areas (exclusion and limited areas) to ensure stringent access control. It involves exchanging one or more identification media (badges, passes, etc.) for another separate type of identifier (badges, passes, etc.).

g. Escort System. Escorting is a method to control visitor personnel within a limited or exclusion area. The escort must remain with the visitor at all times while within the limited or exclusion area. If it is determined by local written policy that an individual does not require an escort within the area, the individual must meet all the entry requirements for unescorted access. Escort personnel may be civilian or military, personnel employed by or attached to the visited activity, and will normally be from the office of the person visited. (For additional considerations on visitor control see paragraph 0505.)

0503. IDENTIFICATION AND CONTROL SYSTEM REQUIREMENTS

The means of identification and control of personnel at an activity will be included in written procedures in the Physical Security Plan and will include the following as a minimum:

6 SEP 1985

- a. Designation of the various restricted areas involved.
- b. Description of the various identification media in use and the authorization and limitations placed upon the bearer.
- c. Identification mechanics for entering and leaving each area, as applied to both authorized personnel and visitors (including movement during off-shift hours).
- d. Details of where, when and how badges will be displayed.
- e. Procedures to be followed in case of loss or damage to identification media.
- f. Procedures to recover issued passes or badges when no longer required.
- g. Procedures to reissue replacements for lost identification. An accurate monitoring system for determining the percentage of lost identification will be instituted. A loss level of six percent is a maximum acceptable standard and the criteria for the reissue of identification should reflect the consideration of the sensitivity of the assets/property being protected.
- h. For those activities where positive access control includes use of card reader access control systems, procedures for removal or invalidation of lost key cards from the system and changes to personnel identification numbers for associated digital key pads (where used) shall be included.

0504. STANDARDS FOR PASSES AND BADGES

a. General. The following considerations are deemed appropriate if a command determines that a pass or badge system of identification is necessary:

(1) An activity's permanent I.D. pass or badge must contain information items set forth in subparagraph b.

(2) A temporary pass or badge need not contain all of the items in subparagraph b (below) since it would only provide control of visitors and personnel who infrequently visit the activity. However, all such badges will be rigidly controlled and accounted for by individual serial number, will be distinctly different in style and design from permanent passes or badges used by an activity and will clearly indicate the period and limits of authorized use.

16 SEP 1985

(3) The activity, installation or host command, as appropriate, may design the pass or badge format. Economy should be a consideration in design. The design agency should bear in mind that the primary purpose of an identification system is to control access to specific areas and alert personnel of the presence of unauthorized persons in the area. Bold print; large, recent photographs; a distinctive design, and tamper resistant structure are prime considerations.

(4) The "exchange badge system" will be employed where security requirements dictate.

(5) The printer's plates for passes or badges will be obtained and safeguarded by the activity to avoid compromise, where possible. When necessary, the pass system may be changed by reprinting in different colors or reformatting the badge.

(6) The activity's badge or pass form will be serialized, controlled and protected.

b. Format/Characteristics. The format/characteristics of a permanent pass or badge are as follows (unless otherwise indicated):

(1) Size which is generally consistent with other standard identification cards.

(2) A photograph. The minimum size is 1" x 1 1/4" (25 mm x 30 mm) (photo size on DD Form 2N). The maximum size will be consistent with economy, available equipment and pass or badge design. The photograph will be in color and stress facial features and not include the area below the neck.

(3) A clear space at the top of the pass or badge to place a hole which will facilitate an attachment device, if required.

(4) A serial number for accountability.

(5) Name of holder, typewritten or printed and incorporated in photo.

(6) Signature of holder.

(7) Rank, rate or grade.

(8) Name, rank and title of validating officer.

(9) Signature of validating officer.

(10) Expiration date of pass/badge.

16 SEP 1985

(11) The following statements are required and may be incorporated in the badge design or be an overlay on the lamination. They may be combined:

(a) "U. S. Government Property."

(b) "Loss of this card must be reported at once."

(c) "If found, drop in nearest U.S. mail box."

(d) "Postmaster: Postage Guaranteed. Return to Commanding Officer, (address of the issuing activity indicated on face of badge)."

(e) "Warning - issued for official use of the holder designated hereon. Use or possession by any other person is unlawful and will make the offender liable to penalty - 18 U.S.C. 499, 506, 701." (Reference should be made to Status of Forces Agreements for overseas activities only).

c. Construction. Security construction requirements will include heat seal adhesion of the complete card which will not allow photographic reproduction. An identifying logo or validation seal or initials will be manufactured into the lamination and other positive security measures which will help prevent tampering. Identifying information must be clearly legible to security personnel at a distance of one meter in normal lighting conditions.

0505. PERSONNEL IDENTIFICATION AND CONTROL PROCEDURES

The following will be provided to establish positive identification and control of personnel entering or departing restricted areas as required by the provisions of Chapter 3 of this manual:

a. Regular Activity Personnel

(1) A method of establishing authority for entry.

(2) A method of establishing identity of personnel requesting entry.

(3) A system to record identity and time of entry and departure of personnel into and out of limited and exclusion areas in accordance with paragraph 0306 of this manual.

16 SEP 1985

(4) A method to ensure positive knowledge of personnel remaining in or entering restricted areas after normal working hours in accordance with the provisions of paragraph 0306 of this manual. Permission for remaining in or entry after normal working hours will only be authorized by personnel who are officially designated by the commanding officer of the activity.

(5) A method to deny access to areas or information to which an individual is not authorized.

(6) A method to recover badges or passes when they are no longer valid.

b. Visitors. For purposes of this instruction, the term "visitor" includes all personnel who require infrequent access to restricted areas or to whom a permanent identification pass or badge for such areas has not been issued. In addition to the actions described in paragraph 0505.a (above), the following will also be considered when establishing local controls for visitors:

(1) Use of a "visitor" pass.

(2) Providing an escort.

(3) Record of area or person visited and authority for entry.

(4) Whether entry or exit administrative inspection has been completed.

c. Contractor Employees. Contractor employees performing work in restricted areas will be required to wear distinctive badges. Use of badges should be considered for contractors in non-restricted areas. In a construction project that will involve a considerable number of personnel over a long period of time, effort should be made to fence off the construction area from the rest of the restricted area. Where the contract work is small, and for comparatively short periods of time, escorts will be necessary if contractor personnel do not have the necessary access authorization.

d. Utility and Maintenance Personnel.

(1) Personnel performing work at infrequent intervals or for a short period within a restricted area will be handled using the same procedures adopted for the control of visitors.

16 SEP 1985

(2) Personnel performing services within a restricted area on a regularly scheduled or full-time basis will be handled using the same procedure adopted for regular activity personnel.

0506. APPLICATION OF PERSONNEL IDENTIFICATION

a. In order for a personnel identification system to be effective, it is important that the guards at control points carefully compare each badge with the bearer and, where a badge-exchange arrangement is employed, the guards make a three-way comparison of the two badges and the individual. To facilitate this comparison process and to affect badge exchanges, ingress/egress control points must be structured so that persons move in single file past the guard (where the volume of entries is high, one guard may check two single file lines, alternating his view between them) through a system of barriers, railings, ropes and stanchions, fences or controlled turnstiles. Close administrative supervision and spot checks of personnel charged with checking identification media are necessary.

b. The manufacture, storage, control and issue of identification media will be carefully controlled to minimize the possibility of counterfeiting or theft, to ensure return and destruction upon termination of employment, and to promptly invalidate lost, mutilated or defective badges. Identification media will be controlled by rigid accountability procedures and unissued "blanks" protected in locked containers with the keys or combinations to such containers under strict accountability. Lost badges will be replaced by badges with new serial numbers to facilitate identification of lost badges.

c. Lost Badge Listing. A list of all activity lost badges will be maintained at all manned points of ingress for use by security force personnel to guard against the unauthorized use of a previously reported lost badge by a person attempting ingress. The lost badge list will be updated at least weekly.

0507. ENFORCEMENT OF MOVEMENT CONTROL

a. Enforcement of movement control systems for restricted areas rests primarily with the activity security force. However, it is essential that they have the full cooperation and participation of other military and civilian personnel (see Chapter 9). All personnel in restricted areas will be instructed to consider each unidentified or improperly identified individual as a trespasser and report him/her to their supervisor, the Security Officer or other appropriate authority. Written procedures will be incorporated into the local Physical Security Plan to ensure coverage of these

16 SEP 1985

requirements. Testing of these procedures will be accomplished during activity physical security and antiterrorism drills and exercises of the security force and inspections or other reviews of the physical security function by the activity's next higher command.

b. Consideration may be given to the utilization of OPNAV approved, commercially available access control systems to enhance enforcement of movement controls within a facility. These systems prevent unimpeded access by unauthorized personnel through access points controlled by card readers and meet security record keeping requirements while reducing the number of security personnel assigned to fixed posts.

0508. SECURITY CLEARANCE ON BADGES

The recording of security clearances on badges or passes is prohibited. However, the badge issued to an individual employed in certain restricted areas may indicate by a code that the bearer is authorized access to that area. The disclosure of classified information to any person solely on the strength of badge coding is prohibited.

0509. VEHICLE IDENTIFICATION AND MOVEMENT CONTROL

Identification and control of personnel is related directly to the identification and control of privately owned motor vehicles on-board activities. The authority to determine the type of identification system used for privately owned vehicles is addressed in references (j) and (k). Instructions established should conform with applicable laws of the state or county in which the installation is located. The vehicle identification method used serves only as a rapid means of identifying the vehicle itself as having authority for being operated and parked on the installation. It will not be utilized or construed as a means of identifying the driver or any occupant therein. Identification required of persons traveling in motor vehicles will be the same as that required of a pedestrian entering or leaving an activity.

a. Regular Registration. The DOD decal is a proper method of identifying vehicles owned by installation residents and for vehicles making daily or frequent visits to the installation. Vehicle decals must conform with reference (j). Commanding officers shall establish positive procedures to ensure vehicles bearing valid DOD decals are not sold, traded, or otherwise disposed of with decals intact.

16 SEP 1985

b. Visitor Control. A large card, displayed on the sun visor or the windshield of a vehicle so as not to obscure the driver's vision, may be used as a temporary means of identification for a visitor's vehicle. Such a card is economical and is not ordinarily subject to theft if the vehicle is kept locked when unattended. The visitor auto pass may be printed in several colors so that use of a particular color can be changed periodically to detect unauthorized use. In addition to the administrative information contained on the card, the following warning statement should be included:

"Acceptance of this pass constitutes your consent to inspection of this vehicle and occupants therein by security force personnel when entering, aboard or leaving this station.

Visitors aboard this installation are guests of the Commanding Officer, and as such should conduct themselves in accordance with the limited conditions under which the invitation is extended. Political activities, pamphleteering, speeches, demonstrations, placard/banner displays, or other similar conduct will not be permitted without written prior permission of the Commanding Officer. Persons violating these conditions shall have their invitations withdrawn, be removed from the installation, and are subject to prosecution."

c. Commercial Vehicles. Commercial vehicles, including buses, may be authorized entry by permanent registration or visitor control methods. Normal search and identification verification procedures and additional local precautions will be applied to prevent unauthorized material or personnel being introduced into or removed from the installation.

d. Control and Review of Identification Media. A system must be established and records maintained to account for all vehicle identification media both regular and visitor. This system will include a positive method for the return, destruction or expiration of an identification medium when it is no longer authorized for use.

e. Government-Owned Vehicles. The guidance and instructions contained in this chapter as they relate to motor vehicle identification do not apply to government-owned vehicles which are provided with other means of identification.

f. Administrative Inspection of Vehicles. All vehicles on naval installations are subject to administrative inspection according to procedures authorized by the commanding officer. As ordered and directed by the commanding officer, authorized security personnel will, while in performance of assigned

16 SEP 1985

duties, administratively inspect vehicles entering or leaving the installation. Such inspections are deemed reasonably necessary to protect the premises, material and utilities of the installation/activity from loss, damage or destruction. Because important constitutional questions are involved, no person or group may be exempted from, or singled out for, such inspections, and the instruction by commanding officers regarding such inspections shall be coordinated in advance of implementation with the local JAG officials to ensure strict adherence to a structured random inspection pattern. As a minimum, guards must be instructed that incoming persons and automobiles may not be inspected over the objection of the individual. However, those who refuse to permit inspection will not be allowed to enter. Persons who enter should be advised to advance (a properly worded sign to this effect prominently displayed in front of the access point will suffice) that they and their vehicles are liable to inspection while on and upon departure. A person who refuses to submit his/her vehicle to an authorized inspection while aboard or upon departure may be detained long enough to obtain a warrant for search of the vehicle, issuance of a letter permanently barring future entrance to the installation, or such other action as may be appropriate under the circumstances.

g. Honoring of Vehicle Identification. Since military and retired military personnel and certain civil service employees will generally have personal or official requirements to enter nearby military activities in their private automobiles, the honoring of DOD vehicle identification media issued to military personnel by other activities is allowed. Honoring of vehicle identification media is to be based on reference (j).

0510. SPECIAL PRECAUTIONS

Personnel responsible for the accomplishment or implementation of personnel and vehicle control procedures shall at all times be watchful for the unauthorized introduction to or removal from the installation of government property, especially weapons, ammunition and explosive materials. This surveillance shall encompass all personnel and means of transportation without exception, including government, private and commercial vehicles, aircraft, railcars and ships.

16 SEP 1985

CHAPTER 6

BARRIERS AND OPENINGS0600. THE PURPOSE OF PHYSICAL BARRIERS

Physical barriers control, deny, impede, delay and discourage access to restricted and non-restricted areas by unauthorized persons. They accomplish this by:

- a. Defining the perimeter of restricted areas.
- b. Establishing a physical and psychological deterrent to entry as well as providing notice that entry is not permitted.
- c. Optimizing use of security forces.
- d. Enhancing detection and apprehension opportunities for authorized personnel in restricted and non-restricted areas.
- e. Directing and channeling the flow of personnel and vehicles through designated portals in a manner which permits efficient operation of the personnel identification and control system.

0601. TYPES OF BARRIERS

Major types of physical barriers are:

- a. Natural - mountains, swamps, thick vegetation, rivers, bays, cliffs, etc.
- b. Structural - fences, walls, doors, gates, roadblocks etc.

0602. GENERAL CONSIDERATIONS

Physical barriers delay but rarely can be depended upon to stop a determined intruder. Therefore, to be effective, such barriers must be augmented by security force personnel or other means of protection and assessment. In determining the type of barrier required, the following will be considered:

- a. Physical barriers will be established around all restricted areas. The type of barrier to be used will be determined after a study of local conditions as required by Chapter 3. The barrier or combination of barriers used must

16 SEP 1985

afford an equal degree of continuous protection along the entire perimeter of the restricted area. When a section or sections of natural or structural barriers (or the lack thereof) provide a lesser degree of protection, other supplementary means to detect and assess intrusion attempts must be used.

b. In cases of a high degree of relative criticality and vulnerability, it may be necessary to establish two lines of physical barriers at the restricted area perimeter. Such barriers should be separated by not less than 30 feet (9.14 meters) for optimum protection and control. Two lines of barriers will only be used either in conjunction with an intrusion detection system between the fences or on the inside fence, or some other form of alarm system and a security force capable of immediate response. The use of two barriers alone provides little extra protection beyond a few seconds of delay to a determined intruder and may actually be counter productive in identifying the location of high risk items.

c. The perimeter boundaries of all installations will be either fenced or walled and posted to establish a legal boundary. This defines the perimeter, provides a buffer zone, facilitates control and makes accidental intrusion unlikely. It is important that consultation be made with local authorities to ensure that posting of barriers in areas of concurrent or proprietary jurisdiction comply with local or state trespass laws. Additionally, designated restricted areas will be posted as specified in Chapter 3.

d. In establishing any perimeter or barrier, consideration must be given to providing emergency entrances and exits in case of fire; however, openings will be kept to a minimum consistent with the efficient and safe operation of the facility without degradation of minimum security standards.

e. Water boundaries present special security problems. Such areas should be protected by material or structural barriers, and posted. In addition to barriers, patrol craft should be used at activities or installations whose waterfronts contain critical assets, restricted areas, or which are otherwise essential to the mission of the installation or activity. In inclement weather, such patrols cannot provide an adequate degree of protection and should be supplemented by increased waterfront patrols, CCTV, watch towers, sentry dogs, etc.

f. Construction of new security barriers and removal of existing barriers and related work must be approved by the security officer and scheduled to provide continuous security for the activity.

0603. FENCES

a. Chain Link Fencing. Chain link fencing is the type of structural barrier most commonly used and recommended for security purposes and must be used to enclose restricted areas where fencing is required. The following standards apply:

(1) Fabric. The standard fence fabric will be 9-gauge (3.8 mm) zinc or aluminum-coated steel wire chain link with mesh openings not larger than two inches (50 mm) per side and a twisted and barbed selvage at top and bottom.

(2) Fabric Ties. Only 9-gauge (3.8 mm) steel ties will be used. If the ties are coated or plated, the coating or plating will be electrolytically compatible with the fence fabric to inhibit corrosion.

(3) Height. The standard height of a security fence is eight (8) feet (2.4 meters). This includes a fabric height of seven feet (2.1 meters), plus a topguard. Building connections may need to be higher. Fencing 12 feet (3.6 meters) high from the connection point with a building away 12 feet (3.6 meters) from the building is suggested.

(4) Fencing Posts, Supports and Hardware. All posts, supports, and hardware for security fencing will meet the requirements of Federal Specification RR-F-191J/GEN of 22 July 1981. All fastening and hinge hardware will be secured in place by peening or welding to allow proper operation of components, but prevent disassembly of fencing or removal of gates. All posts and structural supports will be located on the inner side of the fencing. Posts will be positively secured into the soil to prevent shifting, sagging or collapse (refer to reference (r)).

(5) Reinforcement. Taut reinforcing wires will be installed and interwoven or affixed with fabric ties along the top and bottom of the fence for stabilization of the fence fabric.

(6) Ground Clearance. The bottom of the fence fabric must be within two inches (50 mm) of firm soil or buried sufficiently (concrete footings or gravel may be used) in soft soil to compensate for shifting soil.

(7) Culverts and Openings. Culverts under or through a fence shall be of ten inch (254 mm) pipe, or of clusters of such pipe or equivalent. Openings under or through a fence will be secured with material equal or greater in strength than the overall barrier.

16 SEP 1985

(8) Fence Placement. No fence will be located so that the features of the land (its topography) or structures (buildings, utility tunnels, light and telephone poles, fire escapes, ladders, etc.) defeat its purpose by allowing passage over, around or under the fence.

(9) Top guards. A top guard must be constructed on all perimeter fences and may be added on interior enclosures for additional protection. A top guard is an overhang of barbed wire or barbed tape along the top of a fence, facing outward (away from protected site) and upward at approximately a 45-degree angle. Top guard supporting arms will be permanently affixed to the top of fence posts to increase the overall height of the fence at least 1 foot (0.3 meter). Three strands of 12 gauge (2.7 mm) barbed wire, equally spaced, must be installed on the supporting arms. The top guard of fencing adjoining gates may range from a vertical height of 18 inches (0.45 meter) to the normal 45-degree outward protection, but only for sufficient distance along the fence to open the gates adequately.

(10) Barriers. Buildings, structures, waterfronts and other barriers used instead of (or as a part of) a fence line must provide equivalent protection to the fencing required for that area. Therefore, all windows, doors and other openings or means of access must be guarded or properly secured.

b. Alternative Fencing. Where a boundary passes through an isolated area (forest, jungle, swamp) that is unpatrolled and where vehicular passage is impossible, the boundaries may be defined with a three or four strand 12 gauge (2.7 mm) barbed wire fence approximately four feet (1.2 meters) high. It will be posted as required in Chapter 3.

0604. WALLS

Walls may be used as barriers in lieu of fences for reasons of historical or ceremonial significance. The protection afforded by walls shall be equivalent to that provided by chain link fencing. Walls, floors, and roofs of buildings may also serve as perimeter barriers.

0605. TEMPORARY BARRIERS

In some instances, the temporary nature of a restricted area does not justify the construction of permanent perimeter barriers. The resulting lack of security will be compensated for by additional security forces, patrols and other temporary security measures during the period of use.

16 SEP 1985

0606. CLEAR ZONES

a. An unobstructed area or clear zone will be maintained on both sides of and between permanent physical barriers of restricted and non-restricted areas. Vegetation about such areas will not exceed 8 inches in height.

b. An inside clear zone will be at least 30 feet (9.14 meters). Where possible, a larger clear zone should be provided to preclude/minimize damage from thrown objects such as incendiaries or bombs.

c. The outside clear zone will be 20 feet (6.09 meters) or greater between the perimeter barrier and any exterior structures, vegetation or any obstruction to visibility. Construction of any new fence enclosing a restricted area having a smaller clear zone must be approved by an exception granted via command channels as set forth in Chapter 1.

d. In those activities where space on government land is available, but the fence does not meet clear zone requirements in its present location, relocating the fence to obtain a clear zone may not be feasible or cost effective. Some alternatives to extending the clear zone would be increasing the height of the perimeter fence, extending outriggers, installing double outriggers, and in some cases installing concertina or general purpose barbed tape obstacle to compensate for the close proximity of aids to concealment or access. Where property owners do not object, the area just outside the fence should be cleared to preclude concealment of a person. All fencing will be kept clear of visual obstructions such as vines, shrubs, tree limbs, etc., which could provide concealment for a possible intruder.

e. Inspections of clear zones should be incorporated with inspections of perimeter barriers to ensure an unrestricted view of the barrier and adjacent ground.

f. In addition to security, these clear zones also provide the safety feature of a 50 foot (15.2 meters) wide firebreak between the activity's areas, structures or storage facilities and the adjoining areas. It is especially important to maintain clear zones during period of high fire risk.

0607. PATROL ROADS

When the patrolled perimeter barrier encloses a large area (arbitrarily a large area is considered one square mile (2.60 square km) or greater), an interior perimeter road in all areas not affected by impassable terrain features must be provided for use of security patrols.

16 SEP 1985

0608. INSPECTION OF BARRIERS

Security force personnel shall check security barriers at least monthly for defects that would facilitate unauthorized entry and report them to supervisory personnel. Personnel must be alert to detect the following:

- a. Damaged areas (cuts in fabric, broken posts).
- b. Deterioration (corrosion).
- c. Erosion of soil beneath the barrier.
- d. Loose fittings (barbed wire, outriggers, fabric fasteners).
- e. Growth in the clear zones that would afford cover for possible intruders.
- f. Obstructions at or on the fence which would afford concealment or aid entry/exit for an intruder.
- g. Evidence of illegal or improper intrusion or attempted intrusion.

0609. PERIMETER OPENINGS

Openings in the perimeter barriers will be kept to the minimum necessary for the safe and efficient operation of the activity. They shall be constantly locked, guarded by the security force or otherwise secured to prevent unauthorized entry or exit. When locked and not under constant surveillance, the locking device used shall provide the same security as the perimeter barrier.

0610. GATES

Gates facilitate the entrance and exit of authorized traffic and control its flow.

- a. Number and Location. Gates will be limited to the number consistent with efficient operations. Such factors as the centers of activity and personnel and vehicular traffic flow inside and outside the area should be considered in locating gates. Alternative gates, which are closed except during peak movement hours, may be provided so that heavy traffic flow can be expedited. When open or operating, all gates will be under security force control. They will provide protection equivalent to the outer fences or barriers of which they are a part when not in use. These gates will be locked to form an integral part of the fence when closed.

16 SEP 1985

b. Inspection. When not in active use and controlled by a guard, gates, turnstiles and doors in the perimeter barrier will be locked and frequently inspected by security patrols. Locks will be rotated at least annually. Security for the keys and combinations to locks on these gates is the responsibility of the security officer.

c. Pedestrian Gates. Pedestrian gates and turnstiles will be designed so that only one person entering or departing may approach the guard at a time. Some channels may be closed between rush hours. Where possible, pedestrian and vehicular gates should be clearly separated.

d. Vehicular Gates. Vehicular gates will be set well back from any public highway in order that temporary delays caused by identification control checks at the gate will not cause traffic hazards extending out onto a public highway. There will also be sufficient space at the gate to allow for spot checks, inspections, searches and temporary parking of vehicles so as not to impede the flow of traffic.

0611. DOORS, WINDOWS, SKYLIGHTS AND OTHER OPENINGS

Building egress doors on the activity or restricted area perimeter will provide the protection commensurate with the requirement for proper protection of the assets accessible through those doors. Windows, skylights and other openings which penetrate the perimeter barrier and have an area of 96 square inches (619.4 square cm) or greater will be protected by securely fastened 9 gauge (3.8 mm) wire mesh, framed and permanently bolted to the structure. Such openings are considered inaccessible to personnel when they are 18 feet (5.4 meters) or more above ground level and 14 feet (4.2 meters) or more distant from buildings, structures, etc., outside the perimeter. Protective screens have the additional value of preventing missiles, such as hand grenades, bombs and incendiaries from being hurled through the windows from outside the perimeter (refer to Chapter 4 of reference (r)).

0612. SEWERS, CULVERTS AND OTHER UTILITY OPENINGS

Sewers, air intakes, exhaust tunnels and other utility openings which penetrate the perimeter or restricted area barrier and have a cross section area of 96 square inches (619.4 square cm) or greater, will be protected by securely fastened bars, grilles, locked manhole covers or other equivalent means which provide security commensurate to that of the perimeter or restricted area barrier. Bars and grilles across culverts, sewers, storm sewers, etc., are a hazard when susceptible to clogging. This hazard must be considered during planned

16 SEP 1985

construction of such bars and grilles. All such installations will be designed to permit rapid clearing or removal of grating when conditions require such action. Removable grates will normally be locked in place.

0613. UTILITY POLES, SIGNBOARDS AND TREES

Utility poles, signboards, trees, etc., located outside of and within 14 feet (4.2 meters) of the perimeter barrier of the activity, present a possible means of illegal entry. To reduce this possibility, the perimeter barrier will be staggered to increase the distance to more than 14 feet (4.2 meters) and may be heightened to the extent necessary to prevent entry. Otherwise, the hazard must be removed. Should these utility poles, signboards, trees, etc., also obstruct the visibility of the guards, they must be at least 20 feet (6.09 meters) outside the perimeter barriers.

0614. VEHICLE BARRIERS

The use of vehicle barriers such as crash barriers, obstacles or NCEL developed reinforcement systems for chain link gates at uncontrolled avenues of approach can limit or prevent unauthorized vehicle access. Refer to Chapter 5, Section 2 of reference (r) for guidance on vehicle barriers.

16 SEP 1985

CHAPTER 7

PROTECTIVE LIGHTING0700. GENERAL

Protective (or security) lighting provides a means of continuing a degree of security during hours of darkness approaching that which is maintained during daylight hours. It increases the effectiveness of security forces performing their duties, has considerable value as a deterrent to thieves and vandals and may make the job of the saboteur or terrorist more difficult. Requirements for protective lighting at an activity will depend upon the situation and the areas to be protected. In the interest of finding the best possible mix between energy conservation and effective security, each situation must be carefully studied. The overall goal is to provide the proper environment to perform duties such as identification of badges and personnel at gates, inspection of unusual or suspicious circumstances, etc. Where lighting is impractical, additional compensating measures must be instituted.

0701. GENERAL PRINCIPLES AND GUIDELINES

Chapter 5, Section 3 of NAVFAC Physical Security Design Manual (NAVFAC DM-13.1, reference (r)) provides general principles and guidelines for exterior protective lighting. These guidelines should be applied by activities when determining protective lighting requirements, including Table 20 (Lighting Specification (Foot Candles)), and Table 21 (Illuminated Area Specification) of reference (r). When protective lighting is installed and used, the following basic principles, in addition to those provided in reference (r), should also be applied to help ensure its effectiveness:

- a. Provide adequate illumination or compensation measures to discourage or detect illegal attempts to enter restricted areas and to reveal the presence of unauthorized persons within such areas.
- b. Avoid glare which handicaps security force personnel or is objectionable to air, rail, highway or navigable water traffic or occupants of adjacent properties.
- c. Locate light sources so that illumination is directed toward likely intruder avenues of approach and provides relative darkness for patrol roads, paths and posts. To minimize exposure of security force personnel, lighting at entry points will be directed at the gate and the guard shall be in the shadows. This type of lighting technique is often called "glare protection".

16 SEP 1985

d. Illuminate shadowed areas caused by structures within or adjacent to restricted areas.

e. Design the system to provide overlapping light distribution. Equipment selection should be designed to resist the effects of environmental conditions, and all components of the system should be located to provide maximum protection against intentional damage.

f. Meet requirements of blackout and coastal dim-out areas.

g. Avoid drawing unwanted attention to the security areas.

h. During planning stages, consideration should be given to future requirements of CCTV and recognition factors involved in selection of the type of lighting to be installed. Where color recognition will be a factor, full spectrum lighting vice single color (low pressure sodium vapor, etc.) should be used.

0702. TYPES OF PROTECTIVE LIGHTING SYSTEMS

a. Continuous. The most common protective lighting system consists of a series of fixed lights arranged to flood a given area of perimeter continuously during the hours of darkness with overlapping cones of light. The two primary methods of employing continuous lighting are glare protection and controlled lighting.

(1) Glare Protection Lighting. Uses lights slightly inside a security perimeter and directed outward. This method is useful where the glare of lights directed across surrounding territory will neither annoy nor interfere with adjacent operations. It is considered a deterrent to a potential intruder because it makes it difficult to see the inside of the area being protected. It also protects security personnel by keeping them in comparative darkness and enabling them to observe intruders at considerable distance beyond the perimeter.

(2) Controlled Lighting. Best used when it is necessary to limit the width of the lighted strip outside the perimeter because of adjoining property or nearby highways, railways, navigable water, or airports. The width of the lighted strip can be controlled and adjusted to fit a particular need, such as illumination of a wide strip inside a fence. This method of lighting often illuminates or silhouettes security personnel as they patrol their routes.

16 SEP 1985

b. Standby Lighting. A standby system differs from continuous lighting insofar as its intent is to create an impression of activity. The lights are not continuously lighted, but are either automatically or manually turned on randomly or when suspicious activity is detected or suspected by security personnel or IDS. Lamps with short restart times are essential if this technique is chosen. This technique may offer significant deterrent value while also offering economy in power consumption.

c. Movable Lighting. A system (stationary or portable) which consists of manually operated movable searchlights, which may be lighted during hours of darkness or lighted only as needed. This system normally is used to supplement continuous or standby lighting.

d. Emergency Lighting. May duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies which render the normal system inoperative. It depends on an alternative power source, such as installed or portable generators or batteries.

0703. PROTECTIVE LIGHTING PARAMETERS

It is not the intent of this instruction to prescribe specific protective lighting requirements. Except for minimum standards described in paragraph 0704, the commanding officer of an activity must decide what other areas/assets to illuminate and how to do it. This decision must be based upon the following:

a. Relative value of items being protected.

b. Significance of the items being protected in relation to accomplishment of the mission of the activity in general and its role in the overall national defense structure.

c. Availability of security forces to patrol and observe illuminated areas.

d. Availability of fiscal resources (to procure and install lighting, and follow-on maintenance costs).

e. Energy conservation.

0704. MINIMUM STANDARDS

a. Unpatrollable fence lines, water boundaries and similar areas need not be illuminated. Where these areas are patrolled, sufficient illumination shall be provided to assist the security force in preventing illegal intrusion attempts.

16 SEP 1985

b. Vehicular and pedestrian gates used for routine ingress/egress will be sufficiently illuminated to facilitate personnel identification and access control.

c. Exterior building doors will be provided with lighting to enable the security force to observe an intruder seeking access.

d. Airfields, aircraft, shipyards, controlled industrial areas, piers, docks, petroleum storage areas, and other mission critical areas will be provided with sufficient illumination to enable the security force to detect, observe and apprehend unauthorized intruders.

e. Protective lighting will be checked daily by the security force to ensure all light fixtures are operational. Inoperative lights will be recorded and referred to the security officer.

f. The security officer will ensure that all reports of inoperative protective lights are given immediate attention and will ensure that corrective actions are taken.

0705. EMERGENCY POWER

Restricted areas provided with protective lighting should have an emergency power source located within a restricted area. The emergency power source shall be adequate to sustain security lighting and communications requirements and other essential services required within restricted areas. Provisions must be made to ensure the immediate availability of the emergency power in the event of failure of the primary source. Emergency power sources should start automatically. Battery-powered lights and essential communications should be available at all times at key locations within the restricted areas in the event of complete failure of both the primary and emergency sources of power. Emergency power systems will be tested monthly and the results will be recorded/logged and maintained for a period of two years or until the next cognizant Inspector General command inspection, whichever is last.

0706. TECHNICAL ASPECTS

a. General. The differences in building arrangements, terrain, atmospheric conditions and other factors necessitate the designing of each protective lighting system to meet the conditions peculiar to each activity or facility.

b. Design. Protective illumination must not be curtailed below the minimum consistent with the requirements of

security. Lack of illumination contributes to increases in loss and vandalism which can more than offset energy costs. In designing a lighting system, consideration shall be given to local conditions at the installation or activity, with efforts concentrated on reducing the amount of energy used to deliver the illumination required by taking advantage of all lighting energy conservation opportunities (LECO).

(1) Evaluate LECO for a proposed lighting system in terms of existing systems in the area and future requirements.

(2) A lighting energy audit should be conducted prior to any change to learn what is installed, condition, energy being consumed, light produced, amount of light needed, etc., to determine which type of lamp (incandescent, fluorescent, mercury vapor, metal halide, high pressure sodium or low pressure sodium) system or systems would be best.

(3) Evaluate new system interactions with existing systems in adjacent areas to determine impact (other light levels, electrical transmission systems, heating and cooling systems, etc.).

c. Wiring System. Multiple circuits may be used to advantage in protective lighting systems. The circuits should be so arranged that the failure of any one lamp will not darken a long section of a critical or vulnerable area. The protective lighting system shall be independent of the activity's lighting system, and be so protected that a fire or disaster will not interrupt the entire system.

0707. PROTECTION - CONTROL AND SWITCHES

Controls and switches for protective lighting systems will be inside the protected area and locked and/or guarded at all times. An alternative is to locate in a central station similar to or as a part of the system used in intrusion detection alarm central monitoring stations. High impact plastic shields may be installed over lights to prevent destruction by stones, air rifles, etc.

CHAPTER 8

INTRUSION DETECTION SYSTEMS

0800. INTRODUCTION

Intrusion Detection Systems (IDS) should be an essential element of any in-depth physical security program. IDS consist of sensors capable of detecting one or more types of phenomena, signal media, annunciators, and energy sources for signaling the entry or attempted entry into the area protected by the system. The design, implementation and operation of IDS must contribute to the overall physical security posture and the attainment of security objectives. IDS are designed to detect, not prevent, actual or attempted penetrations. Therefore, IDS is useless unless it is supported by a prompt security force response when the system is activated.

0801. PURPOSE

IDS are used to accomplish one or more of the following:

- a. Permit more economical and efficient use of security personnel through the employment of mobile responding security forces instead of large numbers of personnel for fixed guard posts and/or patrols.
- b. Provide additional controls at critical areas or points.
- c. Substitute for other physical security measures which cannot be used because of safety regulations, operational requirements, building layout, cost or similar reasons.
- d. Provide insurance against human failure or error.
- e. Enhance the security force capability to detect and defeat intruders.
- f. Provide the earliest practical warning to security forces of any attempted penetration of protected areas.

0802. IDS DETERMINATION FACTORS

The following factors must be considered in determining the feasibility and necessity of installing IDS equipment:

- a. Mission of the activity, installation or facility.

16 SEP 1985

- b. Criticality of the activity, installation or facility.
- c. Threat to the activity, installation or facility.
- d. Location (geographic) of the activity or installation and location of facilities to be protected within each activity or installation.
- e. Accessibility to intruders.
- f. Availability of other forms of protection.
- g. Initial and recurring cost of the system.
- h. Personnel and money savings over expected life of the system.
- i. Construction of the building or facility.
- j. Hours of operation of the facility.
- k. Availability of a security force and expected response time to an alarm condition.

0803. TYPES OF SYSTEMS

There are basically four types of IDS:

a. Local Alarm. In this type of system, the protective circuits and alarm devices actuate a visual or audible signal in the immediate vicinity of the protected area, usually on the exterior of the building. The alarm transmission/communication lines do not leave the building. Response is by local security forces that may be in the area when the alarm is sounded. Otherwise, the security force will only know of the alarm if reported by a passerby or during routine checks. The disadvantage of this type of system is that intruders know exactly when the alarm is activated, and in most cases, can easily elude capture. This type of system should be used only when guards respond to it.

b. Central Station. In this type of system, the operation of alarm devices and electrical circuits are automatically signalled to, recorded in, maintained and supervised from a central station, owned and managed by a commercial firm which has guards and operators in attendance at all times. These personnel monitor the signals of the system and provide the response force to any unauthorized entry into the protected area. Connection of alarm equipment to the central station is usually over leased telephone company lines. The provisions of paragraph 0809a apply.

16 SEP 1985

c. Police Connection. In this type of system, the alarm devices and electrical circuits are connected via leased telephone company lines to a monitoring unit located in nearby civilian police stations. An agreement with the local police department must be arranged prior to establishment of this type of system. The provisions of paragraph 0809a apply.

d. Proprietary IDS Station. This type of system is quite similar to a Central Station operation, except that the IDS monitoring/recording equipment for all IDS systems at the installation is located within a constantly manned security force communications center maintained and owned by the government installation. The installation security force operates and responds to all IDS activation. Connection of the alarm sensor equipment to the security force central monitoring station is normally over leased telephone company lines or by separate cable owned and installed by the installation. This is the preferred IDS system for all naval activities and installations.

0804. IDS DESCRIPTION

Each complete intrusion detection system is comprised of various types of equipment that operate in unison to complete the overall detection function. In addition to the actual sensing devices installed at protected locations, the data generated by the sensors must be transmitted by electrical impulse to control annunciator/display equipment in a centralized alarm annunciating station. Electrical power must be supplied for all items. Each equipment category comprises a complete subsystem and is briefly described below along with its employment.

0805. SENSOR SUBSYSTEM

This subsystem is divided into two areas, depending upon their environmental use:

a. Exterior Sensors. Exterior intrusion detection devices (sensors) should be selected for the best performance under such prevailing local environmental conditions as soil, topography, weather and any other factors that could adversely affect device performance or increase its false alarm (an alarm without a known cause) rate. The detecting devices (sensors) are specifically designed for outside installation and usually used in conjunction with barriers such as fences. Commonly used sensors include those that detect light beam interruption, motion, pressure, vibration, magnetic field distortion, and seismic disturbance (or combinations of these).

16 SEP 1985

b. Interior Sensors. Interior intrusion detection devices (sensors) should be selected and installed to provide the best reliable information to the security force in the shortest possible time. The devices are primarily designed to operate within an environmentally protected area to overcome the security weaknesses in the building/structure, room, etc. Commonly used devices include those that detect motion, light beam interruption, sound (both audible and ultrasonic), pressure, vibration, capacitance change, heat, magnetic field change, penetration and the breaking of an electrical circuit.

0806. DATA/SIGNAL TRANSMISSION SUBSYSTEM

This subsystem integrates the sensors and the control/monitoring capabilities into a complete functioning IDS. The transmission medium is used to send control signals and data between all sensors, control points and annunciator display panels. It may be hard wire land lines, radio frequency link or a combination of both. This vital subsystem is probably the weakest and most vulnerable of the entire IDS and requires protection.

0807. ANNUNCIATOR, CONTROL AND DISPLAY SUBSYSTEM

This subsystem provides equipment for central operational control and monitoring of the IDS. Through this equipment, security force personnel are instantly alerted to the status (alarm, secure or access) of any protected area. This subsystem will, whenever possible, be located in a separate area, closed off from public view, at the security force headquarters. Zone numbers shall be used to designate alarmed spaces, vice building and room numbers.

0808. OPERATING POWER SUBSYSTEM

a. Normal. The power to operate an IDS is usually derived from standard 115 volt AC (alternating current) electrical power available in each protected area and the security force headquarters, except where safety requirements prohibit its use (hazardous storage areas, etc.).

b. Emergency/Back-up. The importance of an IDS's continuous function cannot be overstated. Therefore, each IDS will have an emergency/back-up source of power, in the event of an AC power failure, to ensure the system's continuous operation. This emergency/back-up power source usually consists of batteries which will be of the rechargeable type.

16 SEP 1985

0809. INTERIOR STANDARDS

Interior IDS will be an approved DOD standardized system such as the Joint-Service Interior Intrusion Detection System (J-SIIDS), the AN/GSS-20, or commercial equipment, approved by CNO (OP-09N) as an element of the DOD standardized system. Presently installed IDS, not meeting the standards of this instruction, may continue to be used until replacement is necessary. Waivers/exceptions to use presently installed IDS are not required. Appendix XII is reprinted from ONI-CS-63-1-76 (July 1975), subject: Guide for Security Equipment (canceled). It contains a comprehensive description of J-SIIDS equipment and application.

a. All systems within the Navy will be the "Proprietary" type, except where used in civilian communities (Reserve Centers, etc.). In these instances where there is no government response force available, the system may be the "Police Connection" type (formal arrangements will need to be negotiated with the local civil police to ensure that they will monitor and respond to the system) or "Central Station" type (this will require a lease/purchase and contract with a commercial company that monitors the system and will respond 24 hours a day. Telephone answering services will not be used).

b. Annunciator/monitor/display units will be located at the security force headquarters, monitored 24 hours a day, and a response provided to all alarms. These units will provide an audible alarm and a specific identifying visual alarm for each protected area.

c. All alarm transmission lines between the protected area and the monitoring units will be protected by high security electronic line supervision.

d. All sensors, transmitters, control units and other equipment at the protected area will be physically located within the protected area.

e. Shuntlocks (keyswitches or other mechanisms used to activate and deactivate the IDS) will not be installed outside the protected area. Alarm activation delay devices are available which will allow sufficient time for personnel to exit the protected area after the system has been activated.

f. All IDS equipment which can be opened will be fitted with anti-tamper devices which will initiate an alarm signal when the component housing is opened. The anti-tamper system will be in continuous operation regardless of the IDS mode of operation (access/secure/day/night).

16 SEP 1985

g. An emergency/back-up (secondary) power source will be provided for operation of the IDS. This secondary power source will be provided by an uninterrupted emergency generator, if available, or by batteries. Batteries shall have adequate capacity to maintain proper operation of the system under normal operating conditions for a minimum of 4 consecutive hours in the event of failure of AC power. In calculating the size of batteries, 105 percent of the capacity necessary must be provided and it must be assumed that during the period of operation on back-up power, 5 percent of the detection circuits will be in the alarm mode.

(1) Power supply units will include automatic, constant-potential, solid-state batteries of adequate charge capacity for the purpose required. Charge rate will be constantly tapered. Manually controlled, step-type charging is not acceptable.

(2) Power supplies will be so arranged that: batteries are maintained fully charged at all times when AC power is available; batteries are recharged to 85 percent capacity within 48 hours from an almost fully discharged state; system automatically transfers from AC to battery power whenever the former fails and returns to AC power upon restoration of that power; alarms are not initiated on detection circuits upon transfer from one power source to the other; batteries are prevented from discharging into the chargers during any interruption of normal AC power. Supervisory relays will be installed so that audible and visual signals are created on the monitor/annunciator/display panel upon failure and restoration of normal AC power and all power supplies will be protected against overload by fuses or circuit breakers. A positive indicator will be provided for a blown fuse or a tripped circuit breaker indicating which specific fuse or circuit breaker has blown or tripped.

h. All safety hazards will be identified.

i. Contractor Qualifications

(1) Commercial firms used to install, service and/or maintain intrusion detection equipment and/or security alarm systems must be listed by Underwriters Laboratories (UL) to furnish and install burglar alarms in the city and state in which the installation is to be made.

(2) The commercial firm must also be staffed and equipped to provide maintenance within 24 hours on the systems under consideration by the government.

16 SEP 1985

where alarm activations are ignored. As a result, security may be less than that obtained without an IDS. The more complex an IDS, the more highly skilled and trained the maintenance technician must be. The number of technicians required to maintain an IDS depends upon the system's complexity and reliability, and must consider vacation, sick leave, coverage of more than one malfunction at a time and similar factors. Maintenance can be provided by training government personnel (military or civilian) or by contract. The contracting activity will develop procedures to ensure only appropriately cleared contractor personnel inspect and maintain IDS.

b. IDS Testing Frequency. All IDS systems will be tested at least monthly to ensure systems are functional. Tests shall include temporary interruption of AC power to ensure AC/DC transfer and DC batteries or other alternate power sources are functional.

c. Training. Maintenance problems which result in an ineffective IDS are frequently caused by one or more of the following:

- (1) Maintenance personnel who are not adequately trained or equipped (test equipment, tools, publications).
- (2) System maintenance is not assigned a sufficient priority.
- (3) Insufficient number of maintenance technicians.
- (4) Failure to perform routine preventive maintenance.
- (5) Lack of proper instruction and/or written procedures for security personnel responsible for operating and monitoring the system.
- (6) Failure to maintain a record (e.g., log book) on system tests, maintenance, malfunctions, false alarms and similar elements, for review of performance trends and potential problems. The Navy Facilities Engineering Command (NAVFAC) conducts training courses on maintenance of commercial IDS equipment. Details on these courses may be obtained from Director, NAVFAC Technical Training Center, Public Works Center, Naval Station, Norfolk, Virginia 23511. A NAVFAC maintenance manual, M0302, entitled "Maintenance of Intrusion Detection Alarm Systems" is available.

16 SEP 1985

0813. MISCELLANEOUS

Detailed information on IDS component selection and application; sensor/equipment descriptions and layouts; systems design; installation, maintenance and testing is contained in Appendix XII.

16 SEP 1985

CHAPTER 9

PART ONESECURITY EDUCATION AND TRAINING0900. GENERAL

Every member of the naval service and every civilian employee of the Navy has a security responsibility during and after duty hours. Security consciousness and awareness must be stressed by a continuous, vigorous and forceful security education program.

0901. SECURITY EDUCATION

A security education program will be established at each activity to ensure that all assigned personnel, military and civilian, recognize, understand and carry out their responsibility regarding security.

a. Any security program or system designed to combat the security threats discussed in this manual will prove ineffective unless it is supported by a comprehensive security education program. Security personnel cannot effectively accomplish their mission without the active interest and support of everyone on the installation.

b. Program Considerations

(1) It is obvious from a review of the security threats as presented that a security education program must approach security from a total package, a comprehensive 360-degree viewpoint. It must be concerned not only with physical security measures designed to prevent such purely criminal acts as pilferage; but just as important, with counterintelligence measures designed to provide security of classified intelligence information and materials.

(2) It is also essential that the security education program include all pertinent aspects of the crime prevention and loss prevention programs. Many aspects of these programs have direct personal application to all installation personnel.

(3) The individual and collective concern of every military person and Department of the Navy civilian is involved in protection efforts. Security education must be designed to supplement mission accomplishment and be considered essential to the successful implementation of a physical security program.

6 SEP 1985

(4) An educational program should encourage prompt reporting of security breaches and attempt to:

(a) Reduce security infractions and violations.

(b) Act as a communications feedback for improved protective measures.

(c) Reduce losses of government property.

(d) Reduce vulnerability.

(e) Instill security consciousness, which will solicit potential threat information.

(5) The relationship of both types of security, plus the need for close coordination between the security force and Naval Investigative Service personnel in the formulation and operation of a security education program were considered in preparing this chapter.

c. Program Formulation. To ensure integration of security education, the plan must be developed at the installation level, which will require actions by the major commands. Based upon vulnerability and criticality, statistical data of incidents and criminal information formulation must complement both crime and loss prevention as well as counter-intelligence education efforts.

d. Program Objectives

(1) The objectives of a security education program are to acquaint all personnel with the reasons for security measures and to ensure their cooperation. The assumption by installation personnel (military and civilian) that they are not concerned with security unless they work with classified matter or in a restricted area must be overcome. It must be impressed upon them and be continually reiterated that a locked gate or file cabinet does not constitute an end in itself, but is merely an element in the overall security plan.

(2) A continuous program should be presented to selected audiences (primarily supervisors and other key personnel) on timely and applicable topics to develop and foster a high degree of security consciousness.

e. Educational Requirements. Security consciousness is not an inherent state of mind - it must be acquired. Many people are naive and trusting, and are inclined to accept things at face value. Desirable as these characteristics are, they are not conducive to vigilance or security consciousness.

16 SEP 1985

Structural and mechanical aids to security are valueless without the active support of all personnel. All installation personnel must be made aware of the constant threat of breaches of security and of their individual responsibility to detect and thwart such threats. A continuous and forceful education program provides the constant awareness that successful security demands.

f. Graphic Media Aids

(1) Posters - are effective since they may be large in size, brief and to the point, and impact their message at a glance. Posters should be displayed in locations where the majority of people pass and/or congregate.

(2) Placards - used where attention is necessary and people are expected to loiter and have time to read, such as bulletin boards, telephone booths, vending machines, cafeteria and recreation areas.

(3) Leaflets - are economical and are usually pocket size for easy carrying. Distribution of leaflets should be approved by the commanding officer.

g. Indoctrination. This chapter requires the commanding officer to establish security indoctrination and education programs within his command and ensure the following:

(1) Each individual is indoctrinated and kept proficient in the security procedures applicable in the performance of his/her duty.

(2) All personnel are aware of their security responsibilities.

(3) All newly assigned personnel must be given security indoctrinations. The reading of printed security regulations is not sufficient to ensure complete understanding. Indoctrination should consist of a general orientation on the need for and dangers to security, and the individual's responsibility in preventing infractions. It should include a discussion of those hazards common to all personnel, with emphasis on the dangers of loose talk and operational carelessness. It should define general security measures in effect, such as the pass and badge system, private vehicle control, and package inspection. The security indoctrination an introduction to the subject as applied to the particular installation. Further instruction should be applicable to the individual's duty assignment.

16 SEP 1985

h. Crime Prevention. All security education programs should include materials on the crime prevention programs which are designed to reduce crime, including loss of government property through pilferage. This is done by eliminating or neutralizing factors that cause individuals to commit criminal acts. A security education program, therefore, provides an excellent means of disseminating crime and loss prevention information, and of encouraging the active participation of all personnel in observing and reporting security deficiencies, violations, or hazards of any nature.

i. Program of Instruction. The security officer is responsible for planning/administering an effective program of instruction. Coordination with the installation security manager is essential. Profitable use of the limited time normally available for such instruction demands the techniques of a competent instructor. The security officer should give the more important portions of the instruction. Other competent instructors may be used for less important phases or for phases which concern their areas of responsibility, training, and experience.

(1) Each of the officers listed here can assist in the formulation of the program by contributing materials from their own areas of responsibility, knowledge, and interest. Each can also assist by presenting security briefings within those areas.

- (a) Staff judge advocate
- (b) Chaplain
- (c) Special services officer
- (d) Safety director
- (e) Public affairs officer
- (f) Medical services officer
- (g) Naval Investigative Service representative
- (h) Local police and law enforcement officers

(2) The program should be based on an evaluation of the total security posture of the installation. It should begin with an explanation of the program, its aims and objectives - the WHY.

(3) It should then develop the necessary tools to reach those aims and objectives.

(4) It should proceed to delineate methods of education by which the program will be conducted - through individual and group conferences, meetings, speeches, use of news media, posters, placards, leaflets, etc. - the HOW.

(5) Each program must provide for initial and refresher training. It will also provide for debriefing of appropriate personnel.

(6) The program must, above all, stress the absolute requirement for the support of every individual regardless of security clearance or work assignment.

(7) As a minimum, each program should include materials on any recent incidents of security deficiency or violation, and any areas of laxity or trends that have become apparent in the security posture of the installation.

j. Scheduling and Testing

(1) Frequent short periods of instruction are more effective than less frequent long periods. The ideas contained in four well-planned weekly 15-minute classes are more readily absorbed than those contained in a one-hour lecture once a month - regardless of how well the latter is planned and delivered. Instruction that infringes on the free time of the audience is seldom well received. Short periods of instruction to selected groups are easier to schedule without disrupting the operation.

(2) In any form of instruction, testing serves the dual purpose of keeping the audience alert and indicating the efficiency of the presentation and the total program. Tests do not necessarily involve written answers. In fact, skits and hypothetical situations tend to enliven the instruction. Audience participation in giving consequence or solutions to situations presented will accomplish the same results.

16 SEP 1985

CHAPTER 9
PART TWO
SECURITY FORCE TRAINING

0902. GENERAL

a. The effectiveness of a security force is influenced by the quality of its training program. Effective training depends on leadership, proper organization and efficient use of resources. Minimum training standards are essential to enable security force personnel to perform their duties in a professional manner.

b. This chapter outlines requirements and guidelines for security force training, including law enforcement and physical security, for civilian and military personnel who are members of the security department.

0903. DUTIES AND RESPONSIBILITIES

a. CNO (OP-09N) as the Program Manager for all Navy physical security matters shall:

(1) Be responsible for the overall Navy law enforcement and physical security training program.

(2) Provide technical assistance and guidance to individual commands.

(3) Provide technical assistance and guidance to Commander, Naval Military Personnel Command; Chief of Naval Education and Training, and Chief of Naval Technical Training, for the Master-at-Arms conversion course and other Navy law enforcement and physical security training schools, as appropriate.

(4) Provide guidance in the development of in-service and roll call lesson plans and all other law enforcement/physical security training lesson plans and curricula.

(5) Provide information and guidance to assist commands' security force training program including current law enforcement, physical security trends, developments, court decisions, etc.

b. Commanding officers shall:

(1) Ensure that adequate law enforcement/security training is conducted for all security force personnel, as appropriate, in accordance with this instruction and other applicable directives, instructions, and regulations.

16 SEP 1985

(2) Provide broad mission guidance based on the command's requirements.

(3) Allocate sufficient training resources based on training needs and priorities of subordinate units.

c. Security officers shall:

(1) Be responsible for the overall security force training program at their command.

(2) Ensure that all assigned security force personnel are adequately trained in accordance with this instruction and other applicable directives, instructions and regulations.

(3) Administer the security force training program.

(4) Ensure that adequate resources are available to support the security force training program.

(5) Monitor all security force training, evaluations, exercise programs, records, etc for compliance with prescribed standards.

(6) Ensure security force training documentation/aids are available.

(7) Ensure that adequate time is made available to conduct all necessary security force training.

d. Security Department Training Coordinators shall:

(1) Be responsible for developing and administering the security force training program at their commands.

(2) Develop lesson plans, graphic aids, performance checklists, tests, etc. for all security force training required by this instruction and not already developed by OP-09N.

(3) Prepare long range, quarterly and monthly training plans.

(4) Train all security force personnel assigned to their commands and subordinate units.

(5) Record all security force training within individual members' service records and maintain current training records.

16 SEP 1985

e. Security Department Supervisors shall:

(1) Ensure that all security force personnel under their supervision are adequately trained and qualified to perform their assigned duties.

(2) Provide feedback to the training coordinator with regard to the adequacy of security force training as evidenced by assigned personnel, and make recommendations and suggestions.

(3) Afford law enforcement personnel under their supervision the opportunity, time and resources permitting, to attend advanced, in-service, and other military or civilian law enforcement and/or physical security training.

0904. SCHEDULING TRAINING requires the careful attention of the security officer and the training coordinator to ensure that time allocated is used to the best advantage. The installation mission and security support requirement will, to a degree, dictate scheduling, but preference should be given to scheduling instruction during the normal tour of duty whenever possible.

a. Recommend OPNAV Form 3120-1A be utilized for long range and quarterly scheduling purposes. Instructions for using this form and other training and scheduling forms are in Chapter 8 of OPNAVINST 3120.32A.

b. Command security officers shall prepare long range plans for scheduling and budgeting service schools and training activities. Information and availability of quotas and funds for schools and other administrative matters concerning professional and technical schools may be furnished by the servicing civilian personnel office.

0905. EVALUATION OF TRAINING

Periodic review of instructional material shall be conducted to determine how effectively it has met the security force training requirements specified herein. This assessment is accomplished by internal and external evaluation.

a. Internal evaluation is a continuous process which assesses the trainee's performance and evaluates the effectiveness of instructional material and methods. Internal evaluations will take the form of written and graded practical examinations at the completion of the various segments of instruction.

b. External evaluation determines whether the trainees, upon graduation from a particular course of instruction, can

16 SEP 1985

perform the law enforcement or physical security tasks they were trained to perform and if the tasks being trained are, in fact, required on-the-job. External evaluations will usually take the form of on-the-job critiques of the recently graduated trainees by supervisors and field training officers.

0906. GRADUATION REQUIREMENTS

a. To complete a course of instruction, a trainee must successfully complete each graded segment of that training course by passing a written test for classroom work, obtaining an acceptable grade from the instructor for practical exercises or achieving minimum firing range scores as applicable.

b. For each written examination a trainee must achieve a minimum score of 70 percent. Any trainee who does not achieve at least 70 percent on a written examination will be placed in probationary status and required to take and pass a make-up examination.

c. Each trainee will be permitted to take two make-up examinations. If the trainee fails a third examination, he/she will not be permitted to take another make-up nor be considered to have successfully completed the course of instruction.

d. Each trainee must attain a satisfactory or better rating on each graded practical exercise, e.g., unarmed self-defense, crime scenes, breath testing equipment, radar, etc. If a trainee cannot demonstrate minimal standards of performance in all graded practical exercises, graduation will be denied.

e. Upon satisfactory completion of training, the trainee shall be issued a Navy Certificate of Training for inclusion within the member's training or service record. This does not apply to continuing, in-service, or roll call training.

f. Law enforcement and security certificates of training, citations, diplomas, etc. issued by other departments or agencies, military and civilian, should be included in the member's record.

0907. FIELD TRAINING OFFICER (FTO)

A field training officer (FTO) program shall be established on a collateral duty basis in each command security department. FTOs' functions include evaluating the performance of all recently graduated security force trainees ready to assume their security department duties and responsibilities.

16 SEP 1985

a. FTOs shall be highly qualified security force personnel within the security department who have thoroughly and consistently demonstrated their maturity, expertise, and professionalism during the course of their tenure.

b. FTOs shall complete a weekly evaluation of those recently graduated trainees assigned to them, after which their evaluation will be discussed with the trainee. The trainee will sign his/her evaluation for submission to his/her immediate supervisor.

c. Evaluations shall rate the various law enforcement and security tasks performed by or expected of the trainee on a scale ranging from "not acceptable" through "superior" and shall be conducted for a period of 90 days.

d. FTOs and supervisors shall evaluate the effectiveness of the security force training program, in general, and shall periodically discuss the program with the training coordinator.

0908. RECORDING SECURITY/LAW ENFORCEMENT TRAINING

a. A detailed record of all law enforcement and security training shall be maintained within each civilian and military security department member's training or service record.

b. Records should document, as a minimum, subjects and courses of instruction, instructor's name, dates of completion, hours of instruction, examination results, weapons scores, expiration dates of pertinent certifications, licenses and permits, CPR/first aid, radar (doppler systems), breath testing equipment, etc.

c. The same forms used to schedule planned training are recommended for use to record completed training.

0909. EMERGENCY/CRISIS RESPONSE FORCE TRAINING

All security force personnel will be trained in procedures necessary for the implementation of the law enforcement and physical security portion of the command emergency and disaster contingency plans. This training will include periodic alerts and rehearsals of such procedures, and will include coordination with outside agencies which may be called upon in the event of emergencies beyond the capability of local law enforcement personnel.

0910. EMERGENCY VEHICLE DRIVER TRAINING

All security force personnel who operate emergency vehicles may receive the U.S. Department of Transportation,

16 SEP 1985

National Highway Traffic Safety Administrations' Emergency Vehicle Operator Course (DOT EVOC) training. The Navy Safety Center has a Chief Instructor qualified to train instructors to teach the DOT EVOC (ambulance, police, and fire apparatus). EVOC training should be considered only when personnel and other related resources are available to the Command.

a. The DOT EVOC curriculum consists of:

(1) Course Guide, Instructor Lesson Plans and, Trainee Study Guide entitled "Training Program for Operation of Emergency Vehicles".

b. The instruction curriculum described in the course guide prepares emergency vehicle operators to accomplish safely the major functions associated with driving an emergency vehicle. The four emergency vehicle functions of concern in this course include:

- (1) System Support
- (2) Communications
- (3) Emergency Vehicle Operation
- (4) Contingencies

c. The DOT EVOC curriculum is available from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. Stock numbers are:

(1) Course Guide - "Training Program for Operation of Emergency Vehicles, NSN 050-003-003300-1.

(2) Instructor Lesson Plans - Training Program for Operation of emergency Vehicles, NSN 050-003-00332-8.

(3) Training Study Guide - "Training Program for Operation of Emergency Vehicles, NSN 050-003-00331-0.

0911. SECURITY AND LAW ENFORCEMENT TRAINING COURSE

a. General. Each member of the security force is required to complete Phase ONE and Phase TWO training within 12 months of the date of this instruction (see Appendix XIII). All security force members must satisfactorily complete Phase ONE training within 4 months and Phase Two training within 9 months of date of employment or date they initially became permanent members of the security department. New security force members must satisfactorily complete Phase One training prior to performing independent on-the-job security or law enforcement duties. A firearm will not be issued to any security force member who has not satisfactorily completed the firearm qualifications as set forth in Appendix XIII, Tab A.

(1) Commands must determine the length of time to be devoted to individual subject elements. This determination should be based on subject matter as it applies to overall command needs. Commands will ensure, however, that adequate time is devoted to provide trainees with sufficient knowledge of each subject. Regardless of individual subject time allocations, overall Phase One training must encompass a minimum of 80 hours of classroom and practical exercises. Phase Two training will encompass an additional 80 hours of classroom and practical exercises.

(2) Refresher and supplemental training will be conducted on a fiscal year basis. Subject matter will be determined by the individual command physical security and law enforcement needs.

(3) Personnel who have completed the five or eight week training program at the Federal Law Enforcement Training Center, Glynco, Georgia; military police/security training program at the U.S. Army Military Police School, Ft. McClellan, Alabama, or the law enforcement and security training program at the Navy Security Training Center, Lakehurst, New Jersey are exempt from Phase One and Phase Two training.

(4) Specialized and advanced training necessary for efficient and effective operation of a modern security force should be provided. This training includes, but is not limited to, advanced investigative training, formal locksmith training, intrusion detection system (IDS) training, antiterrorism training, loss prevention training and advanced law enforcement and security training.

(5) Additional security training, designated as Phase Two (Appendix VIII), must include systematic development and reinforcement of skills and knowledge that will enhance the individual's ability to perform more effectively.

(6) Home Study Courses. Security force personnel should keep abreast of professional developments and new techniques through publications, periodicals, and specialized security and law enforcement courses available through military service schools. The Federal Law Enforcement Training Center, Glynco, Georgia, the Army Institute for Professional Development, Newport News, Virginia, and other law enforcement agencies offer excellent home study courses for job and career enhancement.

b. Basic. The basic security force training course of instruction is a study of those basic law enforcement and physical security concepts that new security force personnel should understand and be able to perform upon completion and assumption of their on-the-job duties and responsibilities.

(1) Minimum required training standards, designated as Phases One and Two (Appendix XIII), are established for all security force personnel. The course is designed for both military and civilian security force personnel permanently assigned to the security department.

(a) Civilian employees include those in the GS-083 or 085 series, and those personnel (GS-080 and GS-181X series) that may perform or supervise such duties or functions.

(b) Military personnel include those permanently assigned to the security department, with the exception of rated master-at-arms who have completed the rate training course of instruction.

(c) This training is not for TAD personnel, shore patrol, beach guard, master-at-arms forces, etc. for whom the Orientation/Indoctrination Course contained in reference (q) has been developed.

c. Training Course Presentation. The method of presentation for the security force training course will be classroom lecture, laboratory, and practical exercise.

(1) Classroom Lecture is a training situation in which an instructor presents subject material to the trainee for which the trainee is accountable and tested.

(2) Laboratory training is a training situation in which the trainee practices skills under the guidance and supervision of an instructor.

(3) Practical Exercise is a training situation in which the trainee, under the supervision and evaluation of an instructor, participates in a law enforcement or security related situation or performs a law enforcement or security related skill which is graded. Although physical training is set forth within the final area of instruction, it should commence at the onset of the basic training and continue throughout the entire period. By doing so, it is hoped that the trainee will be rendered reasonably fit in a reasonable amount of time and will continue to stay in shape during his/her tenure with the security department.

0912. IN-SERVICE TRAINING

All law enforcement personnel must continue to be involved in professional education and training programs throughout their tours of duty and careers. Those opportunities for professional development that are presented to security force personnel after completion of basic training and assumption of duties and responsibilities are referred to as "in-service training".

16 SEP 1985

a. In-service training is that training geared to ensure that all on-the-job security force personnel maintain and enhance the knowledge, skills, and expertise required to perform their assigned duties and responsibilities in the highest professional manner possible.

(1) A physical fitness program should be developed and administered as an integral part of in-service training. The training coordinator is responsible for establishing such a program.

b. Roll-Call Training. Another form of in-service training which will be utilized is roll call training. This training is a method of providing job related training adaptable to the subjects that all security force personnel must learn. A 10 to 15 minute period of time before each shift will be allocated for this type training. Roll-call training will be utilized to convey some or all of the following information:

(1) Familiarity with departmental programs and operations,

(2) Knowledge of regulations and departmental guidelines,

(3) Introduction of new field service programs,

(4) Knowledge of recent legislation and judicial decisions that may affect law enforcement or security programs,

(5) Familiarity with the services available through various agencies operating in the military and civilian communities.

0913. AUTHORITY TO ARM SECURITY FORCE PERSONNEL

The authority to arm security force personnel is vested in the commanding officer as provided for by references (n) and (o), or as governed by status of forces agreements or local authority in overseas locations. In the exercise of this authority, the commanding officer will be guided by the provisions set forth in this instruction pertaining to the arming of security force personnel.

a. No person will be armed unless he/she is currently qualified in the use of assigned weapons. In order to qualify, Navy military and civilian personnel performing law enforcement/physical security functions must satisfactorily complete the firearms proficiency training course outlined in Appendix XIII of this instruction.

16 SEP 1985

b. Use of Force. Security force personnel will not be armed until each has received detailed instructions governing the use of force in the performance of duties. Specific instruction governing the use of force will be given annually in concert with firearms qualifying/requalifying and quarterly during firearms familiarization sessions. A system will be instituted whereby security force personnel officially acknowledge an understanding governing the use of deadly force.

0914. FIREARMS PROFICIENCY TRAINING

a. General. This paragraph issues policy and procedures for firearms training, range procedures, safety practices, maintenance, and security of firearms by security force personnel.

b. Training and Qualification

(1) Objective. The objective of firearms training is to ensure that security force personnel are qualified to employ firearms with accuracy and speed, and without hazard to self, co-workers, or other parties. To this end, adequate instruction is to be provided concerning policies, procedures, and regulations governing the carrying, utilization, and safety practices relating to firearms. A program of yearly qualification and quarterly familiarization firearms training is required.

(2) Firearms Instruction and Qualification. All security force personnel authorized to carry firearms shall be given instruction in the policy, regulations, and safety practices set forth in this instruction. Before a firearm is issued to assigned security force personnel, they shall qualify on the Combat Pistol Course (See Appendix XIII, tab A) utilizing issued firearms and receive classroom instruction in safety, policy, liability and use of force.

(3) Annual Firearms Qualification. After initial qualification, security force personnel authorized to carry firearms shall be required to requalify with issued firearms annually while assigned to law enforcement and physical security duties. Immediately prior to each annual firearms qualification session, all security force personnel shall be thoroughly briefed concerning, not only safety procedures, but also security department and Navy policies and regulations concerning the carrying and use of firearms.

(4) Quarterly Firearms Familiarization. Security force personnel authorized to carry firearms shall shoot their firearms (including shotguns) quarterly for familiarization using the course illustrated in Tab A of Appendix XIII of this instruction.

16 SEP 1985

(5) Nightfire Exercise. The Nightfire Exercise is intended to be a substitute for one of the three quarterly familiarization sessions, time and resources permitting. This course of fire is designed to be shot on a regular outdoor range utilizing vehicle headlights. It is readily adaptable, however, to specially equipped nightfire ranges, if available.

(6) Transition Course. The Transition Course is designed to act as a basic security force marksmanship skills development and training course. This course should be utilized in conjunction with other courses outlined in this instruction when the individual shooting those courses exhibits a weakness or weaknesses in marksmanship skills resulting in non-qualification. This course is not meant to be a sidearms qualification course and scoring is done in the form of a "satisfactory" or "unsatisfactory" rating for instructional purposes only.

(7) Failure to Qualify or Regualify. Should any security force personnel authorized to carry firearms fail to qualify or regualify, they shall be given additional instruction and will re-shoot the course until a qualifying score is achieved. Should an individual fail to qualify or regualify after additional instruction and three re-shootings, authorization to carry firarms shall be revoked and a written notice of this revocation shall be made by the security officer and filed within the member's training record. The security officer will determine if the individual will continue to receive remediate instruction to qualify or regualify.

0915. CONDITIONS UNDER WHICH SECURITY FORCE PERSONNEL MAY USE DEADLY FORCE

Deadly force is that force which a person uses with the purpose of causing - or which he knows, or should know, would create a substantial risk of causing - death or serious bodily harm. General guidance on the use of deadly force is contained in reference (n). Its use is justified only under conditions of extreme necessity as a last resort, when all lesser means have failed or cannot reasonably be employed, and only under one or more of the following circumstances:

a. Self-Defense. When deadly force reasonably appears to be necessary to protect law enforcement or security personnel who reasonably believe themselves to be in imminent danger of death or serious bodily harm.

b. Property Involving National Security. When deadly force reasonably appears to be necessary to prevent the threatened theft of, damage to, or espionage aimed at property or information specifically designated in writing by a commander

or other competent authority as vital to the national security; to prevent the actual theft of, damage to or espionage aimed at property or information which - though not vital to the national security - is of substantial importance to the national security; or to apprehend or prevent the escape of an individual whose unauthorized presence in the vicinity of property or information vital to the national security reasonably appears to present a threat of theft, sabotage or espionage. Property will be specifically designated as vital to the national security only when its loss, damage or compromise would seriously prejudice national security or jeopardize the fulfillment of an essential national defense.

c. Property Not Involving National Security But Inherently Dangerous to Others. When deadly force reasonably appears to be necessary to prevent the actual theft or sabotage of property, such as operable weapons or ammunition, which is inherently dangerous to others, i.e., property which, in the hands of an unauthorized individual, presents a substantial potential danger of death or serious bodily harm to others.

d. Serious Offenses Against Persons. When deadly force reasonably appears to be necessary to prevent the commission of a serious offense involving violence and threatening death or serious bodily harm (such as arson, armed robbery, aggravated assault or rape).

e. Apprehension. When deadly force reasonably appears to be necessary to apprehend or prevent the escape of a person reasonably believed to have committed an offense of the nature specified in sub-paragraphs b. and d. above.

f. Escapes. When deadly force has been specifically authorized by competent authority and reasonably appears to be necessary to prevent the escape of a prisoner.

g. Lawful Order. When directed by the lawful order of a superior authority who shall be governed by the provisions set forth herein and by reference (n).

In order to comply with local law, a commander may impose further restrictions on the use of deadly force if in his/her judgement such restrictions would not unduly compromise important security interests of the United States.

0916. ADDITIONAL CONSIDERATIONS INVOLVING FIREARMS

If, in any of the circumstances set forth in paragraph 0915 above, it becomes necessary to use a firearm, the following

16 SEP 1985

precautions will be observed, provided it is possible to do so consistent with the prevention of death or serious bodily harm:

a. An order to halt will be given before a shot is fired. Firing a warning shot is a safety hazard and is prohibited.

b. Shots will not be fired if they are likely to endanger the safety of innocent bystanders.

c. Shots will not normally be fired from a moving vehicle.

0917. PRIVATELY OWNED WEAPONS PROHIBITED

Only Government-owned weapons and standard military ammunition officially issued for on-duty use in the performance of law enforcement/physical security functions may be carried by security force members. The use of privately-owned weapons and ammunition in the performance of assigned duties is strictly prohibited.

a. Off-duty security force personnel are not authorized to store government-owned weapons in private residences, either on or off the installation. Government-owned weapons will only be stored in approved security containers or armories in accordance with reference (e).

0918. CONTRACT GUARD TRAINING

Prior to assigning an employee to perform duties as a security guard, the contractor shall provide at contractor's expense, a formal training program conducted at facilities outside the installation. In addition to other training which may be required, each contract guard shall receive training as outlined in Appendix XIII.

a. Contractors presently performing guard services on board a naval installation or activity under a guard services contract are exempt from training requirements established above until a new contract is negotiated at which time guard training shall be required.

0919. CONTRACT GUARD FIREARMS QUALIFICATIONS AND TRAINING

If armed contract guards are required at naval installations or activities, the contract will so stipulate and prescribe minimum standards in accordance with Appendix XIII, Tab A. No contract guard will bear firearms until written certification of qualification is provided to the Contract Officer's Technical Representative (COTR) by the contractor, the guard has successfully completed training in the use of force/rules of engagement, including provisions prescribed by the state in which the contract is administered.

CHAPTER 10

SECURITY FORCE COMMUNICATIONS

1000. GENERAL

At most large installations, the general purpose communication system is not adequate for security purposes. Therefore, the security force will have its own communications system with direct lines between security headquarters and security elements and an auxiliary power supply and sufficient equipment to maintain continuous 2-way voice communications among each element of the security force. Alternate communications systems are required for use in emergencies to provide for increased communications requirements and to maintain sure and rapid communications throughout the emergency.

1001. PURPOSE

a. Security communications will provide the following:

(1) The means for expeditious transmission of routine and emergency instructions between security headquarters, posts and patrols.

(2) The integration and coordination of security functions.

(3) The efficient and economical use of security forces.

(4) The expeditious transmission of requests for assistance to outside sources in the event of an emergency beyond the capability of the security force to control.

(5) The use of the "10" code or other suitable and uniform radio voice communications system.

b. For purposes of this instruction, security communications include:

(1) All telephone systems (field, local, government and commercial) and all radio systems (portable, mobile or fixed) which can be used by the installation or activity for the purpose of providing rapid and reliable 2-way voice communications.

(2) Key operated electric call box systems dispersed strategically throughout an installation for routine tour reports or summoning emergency assistance.

16 SEP 1985

1002. TYPES OF COMMUNICATIONS SYSTEMS

a. Interior Communications. Interior communications are defined as two-way communications for the exchange of information between two or more points within a security area.

b. Exterior Communications. Exterior communications are defined as two-way communications between a security area and an exterior point or points from which assistance may reasonably be expected in the event of an emergency, and for which contingency plans have been formulated.

1003. GENERAL REQUIREMENT FOR THE USE OF SECURITY COMMUNICATIONS SYSTEMS

a. A reliable communications system is necessary for an effective security system. The type of system must be tailored to the requirements of the security network. Considerations include flexibility, criticality, vulnerability to interrupt, size of the installation, natural terrain obstructions and need for responsive reaction. The communications system is largely subject to local determination but the following are general requirements:

(1) At least two systems of exterior communications, one of which will be radio with either an independent or an emergency source of power.

(2) At least two systems of interior communications covering all important fixed areas, one of which must have an independent power source.

(3) A system of radio communications netting all motor patrols, fixed posts and portable ground stations, provided with either an independent or an emergency source of power. Radio communications equipment must have the capability to switch to an alternate frequency in the event the primary frequency is jammed or inoperable. Portable communications equipment procured for security purposes must have self-contained multiple frequency capability.

(4) A dedicated (tactical) frequency and one dedicated back-up frequency for security forces only.

(5) A duress code (changed at least monthly, immediately if compromised) to alert all security forces of emergency situations.

(6) One central communications and dispatch center for all security forces, shore patrol and crisis response forces.

16 SEP 1985

(7) Adequate physical security protection for communications center.

b. Daily inspections and tests of all communications equipment and circuits will be conducted to insure they are operating properly. Tests will be conducted quarterly under simulated emergency conditions. A record/log of all testing results and action taken to correct discrepancies will be maintained for a period of two years or until the next cogni. Inspector General command inspection, whichever occurs last.

16 SEP 1985

CHAPTER 11

SECURITY DEVICES AND EQUIPMENT1100. GENERAL

This chapter contains information helpful in satisfying specific security equipment requirements and in determining their need. It explains general and specific Navy policies on certain devices and equipment not covered in the preceding chapters and describes their basic characteristics, purposes, and limitations.

1101. VEHICLES

The security force shall be furnished with sufficient vehicles to maintain required patrol standards, respond to alarms and emergencies and to maintain supervision. Each security force vehicle will be well-maintained, have reasonable mileage*, be identified as a security (or police) vehicle, equipped with red and/or blue emergency overhead lights, a rotating spotlight, electronic siren, mobile security force radio, provisions for safely transporting detainees (pickup trucks are not adequate transport vehicles and will not be used by police and other law enforcement personnel as primary patrol or duty vehicles), and where shotguns are carried, an electronic latch shotgun holder with concealed switch. Security vehicles which will be used in or will transit proprietary or concurrent jurisdiction areas on or off station during emergency, law enforcement or patrol operations will conform to local and state requirements for the equipping and certification of law enforcement emergency vehicles.

(* All vehicles of the same generic type (sedan, pickup truck, van, etc.) in use at an activity will be rank ordered according to mileage from least mileage to highest. Vehicles with the lowest mileage will be assigned to security and other emergency service uses).

1102. FIREARMS AND AMMUNITION FOR SECURITY FORCES

The basic weapons issued to civilian/military security force personnel will be the revolver, caliber .38 or the pistol, caliber .45 (or 9MM when available). The use of privately owned weapons while on duty is prohibited. In addition to the above weapons, the security force is authorized such other weapons as the commanding officer determines are required to sustain the security force in case of emergency, riot or other contingency. Depending on the overall security needs of the command, such weapons as automatic and

16 SEP 1985

semi-automatic rifles, shotguns, grenade launchers and pyrotechnic pistols may be considered. The security officer and supervisory personnel will periodically review firearm and ammunition requirements to ensure that the number of weapons and amount of ammunition available is appropriate. (Refer to paragraph 0418f of this manual for small arms/weapons allowance changes.)

a. Ammunition used will be commercial or military manufacture with a standard propellant load and fully jacketed ball design. Non-standard rounds will not be carried or used while on-duty by any security force member. Wadcutter and other target loads/handloads may be used as an economy measure during scheduled qualification and practice firings at authorized firing ranges, but any other use of these rounds is strictly prohibited.

b. The required round for the 12 gauge shotgun issued for security force use is the standard commercial or military manufactured round containing a standard propellant charge and a load of 00 size buckshot. The minimum on-duty issue quantity of shotgun rounds is the number required to load the shotgun initially plus one full reload of the magazine.

c. Ammunition for special purpose weapons will be standard military issue or procurement items.

1103. GUARD TOWERS

a. Placing a guard in a tower increases the range of observation during daylight hours and at night with artificial illumination. However, during inclement weather and blackout, towers lose this advantage and must be supplemented by on-the-ground observation. The inactivity of a guard in a tower tends to lull him/her into a state of boredom and can reduce alertness. On the other hand, mere elevation of the observer has an unnerving effect on a potential intruder.

b. Towers may be mobile and may be moved as required to facilitate observation. For adequate protection of guards, towers will be bullet resistant to waist height in accordance with Chapter 7 of reference (r) "Ballistic Attack Hardening", and be provided with portholes and have trap door entrances. Other tower equipment should include tower circle or alidade (used to determine direction), firearms and binoculars. Movable searchlights should be mounted (i.e., overhead) on the tower directionally controlled from inside the tower building and a diffused lighting system located on the inside near baseboards. If stairs are used for entry, a pressure switch with an alarm should be employed to detect unauthorized use of the stairs and alert the guard. Guards should be rotated at frequent intervals to help ensure alertness. Frequent safety inspections will be made of the structure.

16 SEP 1985

1104. MILITARY WORKING DOGS (MWD)

Dogs utilized by the Navy in physical security work are usually of two types: patrol dogs and patrol detector dogs. The patrol dog team, properly trained and used, can be beneficial to an activity's physical security program. When an activity determines that a MWD program is needed, a request to establish such a program must be forwarded via the appropriate chain of command to CNO (OP-09N). The request must include sufficient information to justify the increase in costs associated with establishing and maintaining a MWD program, such as types of assets to protect, crime rate, base location, topography, threat assessment, population, etc. For detailed policy and guidance on the MWD Program, refer to reference (u).

a. Like other highly specialized items of equipment, MWDs supplement and enhance the capabilities of security personnel. The following are some advantages to incorporating the use of MWDs in an installation's physical security plan:

(1) MWD teams provide a powerful psychological deterrent to potential offenders/intruders.

(2) MWD teams can be used to scout, track, search and observe, in addition to routine patrol duties.

(3) Patrol/explosive detector dogs also have the added advantage of being able to detect explosive devices which may have been secreted by an offender.

(4) The dog's keen sense of smell and hearing enable it to detect the presence of intruders and quickly alert the security force member.

(5) There is less chance of fatality through release of a dog than through the firing of a weapon at an intruder.

(6) Dogs are very effective in detecting intruders during hours of darkness.

(7) Dogs are more effective during inclement weather than security personnel on patrol.

(8) Security personnel are more confident when accompanied by a patrol dog.

b. There are problems inherent in the use of MWDs. Attrition and turnover of personnel trained as handlers reduces the efficiency and cost effectiveness of MWD program. Other problems include:

(1) A break-in period is necessary to facilitate the handler and dog working as a team. Commands should allow for about 30 days of additional training time to cover this break-in period.

(2) Care must be taken to ensure that uninvolved persons are not injured by the dogs.

(3) Facilities for kennels and training areas are usually of special project or MILCON scope requiring long lead time. Construction of kennel facilities requires prior CNO (OP-09N) approval.

(4) Care and maintenance of patrol dogs must be considered in manpower requirements. To maintain the physical fitness required of patrol dogs, periodic services of a veterinarian are necessary. This often poses a problem at small or isolated installations. Special facilities are required for the care and training of patrol dogs which adds to the initial expense of adding dogs to the security programs.

(5) The selection and training of handler personnel has been a problem area. The qualities of the handler dictate, to a great extent, the effectiveness of a patrol dog. Volunteers and personnel who like and understand dogs are not always available as handlers. There may be some morale problem among the handlers as much of the work by patrol dogs is at night or after normal duty hours.

(6) Public relations must be considered when planning for the use of dogs. There is strong feeling on the part of many persons that using dogs for security purposes is not in the best interests of the dogs.

c. Although the above factors must be considered before establishing a patrol dog program, care should be exercised that the value of the patrol dog is not underestimated. Any method of reinforcing available manpower, whether it be weapon, machine or animal should be carefully appraised. Certainly the capabilities of security force personnel will increase in scope when augmented by a properly trained patrol dog. The patrol dog, used in conjunction with other physical safeguards, can be invaluable to the commander's physical security program.

1105. CLOSED CIRCUIT TELEVISION

a. Closed circuit television (CCTV), while not an alarm device in itself, is very useful in physical security operations and is frequently used to complement an IDS. This may be accomplished by placing cameras at critical locations to provide

16 SEP 1985

direct visual monitoring from a particular vantage point. Closed circuit television may be used on gates that are not manned continuously or on entrances to vaults or spaces where materials of security interest are stored. This system normally consists of a television camera, monitor and electrical circuitry. The camera may be remotely controlled by monitoring personnel. Closed circuit television also has application in the assessment of alarms. In this configuration, the CCTV can be triggered automatically or by personnel at the alarm control center and can be used to determine whether response forces should be dispatched.

b. It should be recognized that the effectiveness of CCTV is limited. Constantly monitoring a television screen tends to have a hypnotic effect on the viewer. Other distractions are normally gaps in attention and periods when an individual is otherwise occupied, as when answering the telephone, writing, etc. The effectiveness of a CCTV system can be improved by the addition of motion detectors, whereby any movement within a specific area of vision of the camera will activate an audio and/or visual alarm at the control center. Also a video tape recorder can be added at the control center and installed so that it will be activated automatically by the camera's motion detector or by personnel in the control center.

c. Normal use of CCTV on gates must incorporate the use of a two-way communication system between the monitor panel and the gate used in conjunction with an electronically operated gate lock. With this configuration, the person at the monitor panel can be alerted by a person desiring entry, converse with the person using a speaker system, observe the individual on the monitor to determine authority to enter and then, if appropriate, release the gate lock. An adaptation may be added to this equipment to enable security force personnel to make a side-by-side comparison of a person's face with the picture on that individual's identification badge. CCTV thus can be used to minimize the number of security personnel who would normally be needed for gate checking identification.

d. CCTV controls should be enclosed in a metal housing and properly secured to preclude any attempted adjustment by unqualified or unauthorized personnel. The delay caused by the time required for the camera to warm up and be properly adjusted may be eliminated by keeping the camera in continuous operation. Other features which should be considered for inclusion are:

- (1) 360 Degree Pan.
- (2) 90 Degree Tilt
- (3) Automatic Scanning.

16 SEP 1985

- (4) Zoom Lens.
- (5) Telephoto Lens.
- (6) Color TV (high cost as compared to black and white).
- (7) Emergency Power Back-Up.
- (8) Fast Warm-Up Capability.
- (9) Remote Adjustment.
- (10) Special Environmental Enclosures.
- (11) Moving Image Sensor.

e. A common problem with CCTV systems is the light intensity required for available cameras. This requirement must be determined, and the availability of sufficient light verified, before the system is purchased and installed. Other problems which must be considered are the initial cost of the system, the cost of maintenance, weather conditions that may hamper the visibility of the guard making a positive identification of badges and proper installation.

f. Double gates or entrapment entry systems wherein the person is contained between the two gates until positive identification is made can help reduce the probability of a forced entry and should be complemented by use of CCTV to establish positive personal identification.

g. If used, CCTV maintenance contracts shall include wording, in effect, as follows: "When removal of a system component is necessary, the contractor shall be fully responsible for any loss or damage. A loan of the same type component, operable within the CCTV system, shall be furnished by the contractor within four working hours after removal of the system component to be repaired, without additional cost to the government. Also without adding cost to the government, the contractor shall be responsible for maintaining this replacement component in a totally functional condition until the repaired component is returned and made to operate in a totally functional manner within the system".

1106. WATER PATROL CRAFT

Patrol craft should be equipped with at least one searchlight, a public address system, special emergency equipment, be specifically designated as a security vehicle, be provided continuous two-way radio voice communication capability with individual units ashore and the central security dispatcher, and be so constructed as to afford seaworthiness and protection against inclement weather and sea conditions. Sonar/radar and night vision devices are encouraged.

1107. SECURITY FORCE EQUIPMENT

There are numerous devices and/or specialized equipment

security program. Security officers and supervisors shall obtain such equipment as may be necessary to improve their security program. Items in this category will include, but are not limited to, warning lights, sirens, portable lights, flashlights, portable radios, first aid kits, traffic control devices and special clothing for the health, comfort, or safety of security personnel. Security officers and supervisors must keep abreast of new equipment to improve the effectiveness of the security program.

1108. SECURITY FORCE INDIVIDUAL EQUIPMENT

All security force individual equipment (yellow rain slickers, radios, riot control gear, helmets, holsters, belts, handcuffs, flashlights and batteries, etc.) other than personal headgear, clothing, and footwear, will be procured by the Navy activity and issued to its civil service or military security force members.

16 SEP 1985

APPENDIX I

REFERENCES

- (a) OPNAVINST 5510.1G, Subj: Department of the Navy Information and Personnel Security Program Regulation
- (b) OPNAVINST S5460.4C, Subj: Control of Special Access Program within the Department of the Navy (NOTAL)
- (c) OPNAVINST 5239.1A, Subj: Department of the Navy Automatic Data Processing Security Program
- (d) OPNAVINST C5510.83E, Subj: Navy Nuclear Weapon Security Manual
- (e) OPNAVINST 5530.13, Subj: Department of the Navy Physical Security Instruction for Sensitive Conventional Arms, Ammunition and Explosives (AA&E)
- (f) SECNAVINST 5500.4D, Subj: Missing, lost, stolen, or recovered Government property; reporting of
- (g) SECNAVINST 5511.36, Subj: Authority of Military Commanders under the Internal Security Act of 1950 to Issue Security Orders and Regulations for the Protection or Security of Property or Places under their Command
- (h) SECNAVINST 5822.1, Subj: Federal Magistrates Act; Implementation by Department of the Navy (NOTAL)
- (i) OPNAVINST 5102.1A, Subj: Mishap investigation and reporting
- (j) OPNAVINST 5560.10B, Subj: Standard procedures for registration and marking of non-government-owned motor vehicles
- (k) OPNAVINST 11200.5B, Subj: Motor Vehicle Traffic Supervision (NOTAL)
- (l) SECNAVINST 5530.4, Subj: Marine Corps Security Force (MCSF) barracks and detachments ashore and afloat (NOTAL)
- (m) SECNAVINST 5520.3, Subj: Criminal and security investigations and related activities within the Department of the Navy
- (n) SECNAVINST 5500.29A, Subj: Use of force by personnel engaged in law enforcement and security duties

OPNAVINST 5530.14A

16 SEP 1985

- (o) SECNAVINST 5500.32, Subj: Carrying of firearms by personnel of the Department of the Navy
- (p) OPNAVINST 5530.15, Subj: Physical Security
- (q) OPNAVINST 5580.1, Subj: Navy Law Enforcement Manual
- (r) NAVFAC DM-13.1, Subj: Physical Security Design Manual
- (s) OPNAVINST 3850.4A, Subj: Protection of Department of the Navy Personnel and Resources Against Terrorist Acts.
- (t) SECNAVINST 5820.7, Subj: Posse Comitatus Act
- (u) OPNAVINST 5585.2, Subj: Navy Military Working Dog Program

OPNAVINST 5530.14A

16 SEP 1985

- (o) OPNAVINST 5100.12A, Subj: Navy traffic safety program; promulgation of
- (p) OPNAVINST 5102.1A, Subj: Mishap investigation and reporting
- (q) OPNAVINST 5130.1A, Subj: Armed Forces Courier Service Charter
- (r) OPNAVINST 5130.2A, Subj: Armed Forces Courier Service Administration and Operations
- (s) OPNAVINST 5310.12E, Subj: Shore Required Operations Capability (SHOROC) (NOTAL)
- (t) OPNAVINST 5585.2, Subj: Navy Military Working Dog Program
- (u) OPNAVINST C5500.46B, Subj: Technical Surveillance Countermeasures (U) (NOTAL)
- (v) OPNAVINST 5510.48H, Subj: Manual for the Disclosure of Classified Military Information to Foreign Governments and International Organizations
- (w) OPNAVINST 5513.1B, Subj: Department of the Navy Security Classification Guidance
- (x) OPNAVINST 4650.11D, Subj: Official temporary duty travel to military and civilian installations, activities, and units; policy and procedures for
- (y) OPNAVINST S3820.16C, Subj: Foreign Military Intelligence Collection Activities (FORMICA) (U) (NOTAL)
- (z) OPNAVINST 5540.8H, Subj: DOD Industrial Security Program (NOTAL)
- (aa) OPNAVINST 5560.10B, Subj: Standard procedures for registration and marking of non-government-owned motor vehicles
- (bb) OPNAVINST 11200.5B, Subj: Motor vehicle traffic supervision (NOTAL)
- (cc) OPNAVINST 5510.1G, Subj: Department of the Navy Information and Personnel Security Program Regulation
- (dd) OPNAVINST C5510.83E, Subj: Navy Nuclear Weapon Security Manual (U)

- (ee) OPNAVINST 5530.13, Subj: Department of the Navy Physical Security Instruction for Sensitive Conventional Arms, Ammunition and Explosives (AA&E)
- (ff) NAVINVSERVINST 5520.22, Subj: Barricaded Captor/Hostage Situations (NOTAL)
- (gg) NAVMATINST 8300.1A, Subj: Small Arms and Weapons Management Program; policy and guidance concerning (NOTAL)
- (hh) OPNAVINST 5580.1, Subj: Navy Law Enforcement Manual

APPENDIX III
PART 1

SABOTAGE - ITS DETECTION AND PREVENTION

1. THE SABOTAGE THREAT. In the context of federal criminal law, sabotage refers to the willful obstruction of or interference with defense activities (18 U.S.C. 2151-56). It includes such things as: willfully injuring, interfering with or obstructing the United States or any associate nation, in their preparing for or carrying on of defense activities; willfully making or constructing, in a defective manner, any material or tools used in making war material.

a. The highly effective results which may be accomplished by the skillful employment of sabotage, as well as the known existence of certain groups available and willing to undertake such work, places this hazard high on the list of risks confronting the Navy. In terms of trained manpower, equipment and risk, a sabotage operation involves only negligible expenditure by the enemy; but the profit may be enormous if a target has been strategically selected.

b. The greatest danger of sabotage lies in concerted, simultaneous covert sabotage attempts against sensitive military installations or facilities, which, if successful, could seriously jeopardize military operations and could prevent commanding officers from performing combat missions. It is a threat of sabotage that requires sabotage alert procedures to be an important part of physical security plans.

c. Sabotage as a diversion measure:

(1) Sabotage, particularly in the form of fire or mine explosions, may also be used as a diversion to permit pilferage by drawing attention to the affected area and away from the object of the pilferage.

(2) This hazard exists particularly when security personnel are also responsible for firefighting and similar control operations.

d. The sabotage statutes (18 U.S.C. 2151-56) are concerned with acts intended to impede our war-making capability. However, security personnel have a broad responsibility for protecting U. S. government property. Security personnel should be alert to any act which intentionally or maliciously destroys or damages U. S. government property or disrupts the operation or mission of an installation or facility (whether or not it be prosecuted under the sabotage laws). This includes vandalism and malicious mischief (18 U.S.C. 1361-63); (UCMJ, art. 108)

16 SEP 1985

2. RECOGNIZING SABOTAGE. Recognition of an act of sabotage is often difficult, because the ultimate target may not be readily apparent and the act itself frequently destroys all evidence of sabotage. To employ effective countermeasures against the threat of sabotage, it is necessary to understand some of the methods and targets of the saboteur.

3. CHARACTERISTICS OF SABOTEURS

- a. May be highly trained professionals or rank amateurs.
- b. May be computer programers, laborers, machinists, flight engineers, foremen, or members of management.
- c. May be specially trained enemy agents assigned a specific mission or individual enemy sympathizers, or disaffected natives who act for their own personal reasons or interests.
- d. May work alone or in groups. They may infiltrate military or industrial groups as legitimate members, or they may work from the outside.
- e. May or may not have affiliation with foreign or military groups.
- f. May be discontented employees.
- g. May be very vulnerable to subversive propaganda.
- h. May be mentally ill.
- i. Act on impulse.

4. CHARACTERISTICS OF ENEMY SPECIAL AGENTS

- a. Directed, trained, supported, and supplied by a subversive organization.
- b. Coordinate efforts in an overall attempt to impede or disrupt industrial potential.
- c. May lie dormant for years awaiting desired opportunity.
- d. The motivation of an enemy special agent or an enemy sympathizer is obvious. The motivations of disaffected natives are much more complex. Correspondingly such agents are more difficult to detect, and individual motives may be as varied as the personality.
- e. Agents may work for pay, hatred, revenge, sincere beliefs, blackmail purposes, or settling real or imaginary grievances.

5. SABOTAGE TARGETS. In choosing targets, saboteurs are influenced by two basic considerations analogous to those found in a tactical situation; namely, the objective, and how best to attain it. Is the destruction of the target to be sufficient in itself, or is it but a contribution to a larger plan? The ultimate in sabotage is complete and permanent destruction of the target. When this cannot be attained there may be many lesser targets, and enough of these strategically grouped may achieve comparable results.

6. TARGET ANALYSIS. In analyzing a sabotage target, the saboteur considers the following factors:

a. The importance of the installation or facility from a technical or military standpoint. Will its complete or partial destruction hinder or breach the overall defense?

b. When complete destruction is not possible, what specific items of technical or military importance will have the most crippling effect on the mission of the installation? For example:

- (1) Rail yards and train equipment.
- (2) Transformers at power stations.
- (3) Dies in machine shops.
- (4) Pumps at waterworks and pumping stations.
- (5) Condensers at steam power plants.
- (6) Fuel pipelines.
- (7) Weapons and ammunition storage points.
- (8) Airfields and airstrips and their facilities.
- (9) Nuclear refueling facilities.
- (10) Significant communications modes.

c. The capability of a target for self-destruction is always attractive to a saboteur. Heavy rotating machinery, such as turboelectric generators, can be ruined by a disturbance of the shaft alignment or by placing abrasives in the lubrication system. Other examples of self-destroying targets include ammunition and gasoline dumps, dams, caissons, and warehouses containing inflammable stocks.

7. METHODS OF ATTACK. The following specific targets are vulnerable to one or more methods of sabotage:

16 SEP 1985

a. Natural Resources

(1) Mines may be sabotaged by causing cave-ins or flooding of the shafts or tunnels.

(2) Forests may be destroyed by incendiaries; while fruit trees may be killed by an induced blight.

(3) Farm produce is vulnerable to parasites and various blights, and by the diversion of water used for irrigation.

b. Army, Navy, Marine, and Air Force Installations or Facilities. Any action against an armed forces installation or facility, which disrupts or prevents full accomplishment of its mission, constitutes a potential threat. Sabotage actions intended to destruct ammunition or fuel supplies, and to disrupt communications are common to all of the armed services. Other targets are peculiar to each service, such as drydocks and repair facilities to the Navy, and complex flight and navigation equipment to the Air Force. Headquarters buildings and billets located outside the installation or facility are specific targets of terrorists and insurgents, especially by bombing and arson.

c. Industrial Facilities. Industrial and production facilities present innumerable possibilities for explosive and mechanical sabotage, and are especially vulnerable to acts that will initiate a chain reaction. The following are examples of means by which sabotage can be committed in industrial and production facilities:

(1) Drainage of oil or blocking of lubrication pipelines.

(2) Introduction of abrasives into machinery.

(3) Missetting or damaging process control instruments.

(4) Introduction of small tools or other pieces of metal into moving gears.

(5) Explosive charges placed to have a shattering effect when detonated.

d. Warehouses and Supply Depots. Material in storage is subject to ordinary explosive or incendiary sabotage. There is also an opportunity for delayed sabotage by the introduction of abrasives, contaminants, or adulterants into the items stockpiled. This latter type of sabotage will not normally be discovered until the material is put into use, and is difficult to detect or trace.

e. Transportation. The propelling machinery and cargoes of land, sea, and air transportation are subject to acts of sabotage similar to those mentioned in paragraph c above. In addition, rail transportation can be sabotaged by damaging switches, rails, roadbeds, and various structural adjuncts, such as bridges, tunnels, and shop facilities.

f. Materials In transit. Supplies or equipment of any type in transit may be sabotaged, either by destroying the means of transportation or by directly attacking the materials, or both. A bomb or arson device placed in the hold of a ship may damage or destroy both the cargo and the ship. A bomb or arson device used against a railroad tank car may destroy the car, its contents, and a portion of the rail line. The same applies to petroleum pipelines.

8. SABOTAGE METHODS. There are many ways to commit sabotage, and new methods and devices are constantly being adopted.

a. A major sabotage effort may be undertaken after a thorough study of the physical layout of the facility and its production processes by technical personnel fully qualified to select the most effective method to strike one or more of the most vulnerable parts of the facility.

b. Sabotage may, on the other hand, be improvised by the saboteur, relying solely upon his own knowledge of the facility and the materials available to him. The device or agent selected for sabotage may range from the crude or elementary to the ingenious or scientific.

c. The methods of sabotage may be classified as follows:

- Fire
- Explosive devices
- Mechanical devices
- Chemical
- Psychological

9. SABOTAGE BOMBS. An explosive bomb itself is the unit of destruction and is not dependent upon outside aid as is an incendiary bomb; it is, therefore, normally larger than an incendiary bomb. However, the same ingenuity of disguise is applicable as in the case of an incendiary bomb.

a. Five sticks of dynamite taped together and equipped with a blasting cap would make an effective bomb, but upon sight would incite suspicion and concern. The same five sticks of dynamite stuffed in a suitcase with a drycell battery and a clock-work delay device would be just as destructive, but would not attract attention.

16 SEP 1985

b. A lump of plastic explosives coated with a mixture of shellac and coal dust would be unnoticed in a load of coal. The possible combinations of explosives, activator, delay device, and outside containers are many.

10. BOMB HANDLING. In any discussion of the handling, disarming, or disposal of sabotage bombs, it must be realized that the exterior appearance of a known or suspected bomb gives little or no indication of the explosive used or the manner of construction. Both of these key factors are largely dependent upon the availability of materials and the technical skill of the saboteur.

a. In view of the infinite varieties possible, it is obvious that no set procedure can be established for their handling. However, the primary consideration is the safety of life and property, and there are certain basic rules which must be followed.

b. Wherever the possibility of a sabotage bomb exists, there must be a pre-arranged plan for coping with such an emergency so that the following steps may be carried out quickly and in many cases concurrently:

(1) Clear the area of all personnel, cordon the area, and establish a guard control around the danger zone.

(2) Send for technical help such as a local military or civilian explosive ordnance disposal team.

(3) Immediately notify the Security Officer.

(4) Shut off power, gas, and fuel lines leading into the danger area.

(5) Notify the fire department, medical service, Naval Investigative Service, Federal Bureau of Investigation, as appropriate.

(6) Secure mattresses or sandbags for use as protective shields and barricades. Sandbags may also be used in confining and directing the force of an explosion.

(7) Remove flammable materials and small objects from the surrounding area. However, anything that might be connected with the bomb or might act as a trigger mechanism must not be touched.

(8) Arrange for the use of portable X-ray fluoroscopic equipment, which will be used by technical personnel only.

11. COUNTERSABOTAGE. Countermeasures against sabotage include, but are not limited to, the following:

- a. Planning
- b. Employee education
- c. Risk analysis and evaluation
- d. Protective barriers
- e. Identification and movement control systems
- f. Searches of incoming vehicles
- g. Restricted areas
- h. Safeguarding classified information
- i. Investigation of security breaches
- j. Physical security surveys and inspections
- k. Of utmost importance is the building and maintaining of employee morale, informing employees of threatened dangers, how they may be recognized and what protective measures are available.

16 SEP 1985

APPENDIX III

PART 2

ESPIONAGE - RECOGNITION AND PREVENTION

1. ESPIONAGE. What is espionage?

a. JCS Pub 1 appropriately defines espionage as actions directed toward the acquisition of information through clandestine operations. Each member of the Navy is a potential target for espionage activities. Each member of the Navy possesses knowledge of some importance the enemy would like to know, or is regarded as a possible source of information. This information is desired for the following reasons:

(1) To determine the progress of the United States in the area of national defense.

(2) To compare weapons, equipment, techniques, and devices with their own.

(3) To use data to advance their own scientific or weapons achievement.

(4) To assist with sabotage efforts.

2. WHY ESPIONAGE? In the United States the industrial organization of the nation is the center of economic life in peace, and the indispensable arsenal of the country's fighting forces and those of U.S. allies in war. When there are serious disruptions in the industrial structure, the effects are widespread.

a. Espionage, as discussed here, is the action of spying on a country - that is, of secretly or under false pretenses, searching out information, or making observations with the intention of relaying the information or observation to another country (18 U.S.C. 792-98).

b. Wartime disorder in the industrial world can mean the difference between victory and defeat. Wartime disruptions can be caused by peacetime espionage. Of more immediate interest to security force personnel is the fact that espionage is a mandatory prerequisite to enemy agent sabotage of the type and scope discussed in Part 1 of this Appendix.

c. It is imperative that commanding officers, physical security personnel, and others responsible for security of naval installations and industrial facilities, understand the possibilities of espionage and insure that security forces are properly trained and always on alert for the espionage agent and his methods.

(1) Such collection of information contributes to an evaluation of a nation's war potential and can be used to advantage in sabotage or in case of armed attack.

(2) Espionage activity exists on a massive worldwide front, and the United States is threatened by this type invader.

(3) Even during times of peace, espionage agents seek scientific, economic and military information.

d. Espionage has played a vital role in keeping many foreign powers abreast of developments in the scientific and technical fields.

3. SOURCES. With the exception of so-called low-level agents, espionage agents are normally well selected and highly trained. A typical high-level agent is subtle and tactful and is usually skilled in applied psychology. The typical agent today is more likely to appear in the guise of an ordinary individual fitting into the local area and situation.

a. Espionage organizations may develop data piecemeal, through contributions of many agents whose fragmentary reports fit together like pieces of a puzzle to complete a precise picture of a military installation or industrial facility.

b. Espionage agents may be expected to use great ingenuity in obtaining information. Some of the methods which they may employ are:

(1) Stealing or purchasing information from employees.

(2) Stealing information from records or other sources.

(3) Using various means of reproducing documents, products, processes, equipment, or working models.

(4) Using a "front" such as commercial concerns, travel agencies, import/export associations, scientific organizations, insurance agencies, businessmen's groups, and other organizations to obtain confidential information or pertinent statistical information that can be translated into strategic information.

(5) Using blackmail techniques by threatening to expose intimate and personal details concerning an individual.

(6) Using threats of danger to friends or relatives of an employee to obtain information.

(7) Using various means to skillfully extract information from members of the family or close friends of an employee.

(8) Obtaining information at social gatherings.

(9) Gaining information by personal observation of production operations, test runs, shipment of finished product, or confidential papers.

(10) Securing information from waste and carbon paper and other discarded records.

(11) Attempting subversion by offers of money or by playing on the emotions, such as love, hatred, desire for power, etc.

c. The easiest and least dangerous method by which an agent can gain information is to listen to loose talk. Many individuals have a tendency to talk about security matters with little regard for the consequences (thinking that security is useless anyway).

4. WHAT DO THEY WANT? Espionage agents will attempt to obtain any information which contributes an evaluation of the nation's war potential and which may be used to advantage by an enemy in sabotage activities, subversive activities, and armed force attack. Espionage agents may initially request innocuous information, such as the plan of the day, an installation phone book, etc. If the "targeted" individual provides such information, the espionage agent may escalate the sensitivity of information requested until the target is deeply involved and feels he/she must provide the information or risk being exposed. Some of the specific subjects in which espionage agents may be especially interested include:

a. Strength, location, disposition, movement and combat efficiency of U.S. and allied warships.

b. Capacity, rate of production, industrial mobilization schedules, and details of orders on hand.

c. Specifications of products or special equipment and methods of operation.

d. Test records of newly developed items or equipment.

e. Sources of raw materials and components.

f. Inventory of completed products, destination, and transportation means and routes.

16 SEP 1985

- g. Data on production or testing methods.
- h. Critical and vulnerable points and possible methods of effective sabotage.
- i. Measures in force for security to prevent sabotage, such as location of security posts and mobile patrols.

5. CONTROL MEASURES. Primary responsibility for investigation of subversive activities and for counter-espionage operations rests with the Naval Investigative Service and Federal Bureau of Investigation.

a. It is important that physical security personnel understand that they are to report immediately any suspicion or evidence of subversive elements. They must not conduct investigations on their own. Months of hard work on the part of counterintelligence personnel may be ruined by the thoughtless actions of one security guard.

b. The primary objective of physical security personnel with respect to espionage is to render it ineffective, or at least to make it more difficult by applying protective measures.

c. Some of the security measures that may reduce the degree of risk from espionage include:

- (1) Personnel security investigations and careful loyalty checks of personnel, particularly before employment.
- (2) Prevention of unauthorized entry to the premises of the installation.
- (3) Proper consideration to classification of military information, and special guarding, careful handling, and safekeeping of classified material.
- (4) Controlled burning of waste paper, carbons, and typing tape connected with the preparation of classified material.
- (5) Restriction of movement of all personnel within the installation.
- (6) Continued evaluations of human weaknesses of personnel having access to classified or sensitive information.
- (7) Continued orientation, education and security information programs of the types prescribed in this instruction.

APPENDIX III

PART 3

BOMB THREATS

1. Bomb threat planning is an important facet of any physical security program (plan), whether for a single building, a facility, or an installation. This Appendix provides the security officer a basic outline from which he can develop an effective bomb threat plan and training program. The purpose of this appendix is to provide outline guidance in planning for or responding to bomb threats.

a. A bomb is a device capable of producing damage to property or death to personnel when detonated or ignited. Bombs are classified as explosive or incendiary. An explosive bomb causes damage by fragmentation, heat, and blast wave. The heat produced often causes a secondary incendiary effect. An incendiary bomb generates fire-producing heat without substantial explosion when ignited. Bombing occurs when an explosive bomb detonates, or an incendiary bomb ignites.

b. A bomb threat is a message delivered by any means which may or may not:

(1) Specify location of the bomb.

(2) Include the time for detonation/ignition.

(3) Contain an ultimatum related to the detonation/ignition or concealment of the bomb.

c. A bomb incident involves any occurrence concerning the detonation/ignition of a bomb, the discovery of a bomb, or receipt of a bomb threat.

3. Countermeasures. Measures taken to minimize the production and placement of bombs to include reducing the disruptive effects are as outlined:

a. Preplanning considerations.

(1) Preplanning is an essential prerequisite for developing a workable bomb threat plan. In the preplanning phase, provision must be made for:

16 SEP 1985

- Communication channels
- Support organizations
 - Primary
 - Alternate

(2) Communication equipment. Do not operate radio transmitters in the vicinity of the device. They could detonate it. The following elements should have communications capability:

- Emergency operations center
- Facility/area inspection
- Reporting system
- Search teams
- Security teams

b. Prepare the bomb threat plan. Any effective plan must address at least the following considerations:

- Control of the operation.
- Evacuation.
- Search.
- Finding the bomb or suspected bomb.
- Disposal - EOD
- Detonation and damage control. Barricade material around the device to guide device fragments upward.
- Control of publicity.
- Erection of barriers.
- Fire and medical service standby.
- Disconnection of utilities.
- Removal of flammables/explosives.
- After action report.

c. Evaluate the threat.

d. Activate the plan.

4. How to Search. A bomb threat may be received by any of the following:

- Telephone message.
- Suspicious package through the mail.
- Written message through the mail.

a. Search Techniques. The choice of search techniques will depend on whether the threat is overt or covert. The following decisions must be made before the proper techniques can be applied:

or to, after, or without evacuation.
supervisors, occupants, or a special

- Percent of building to be searched.
- If a search team is used, it should be divided as follows:

- Outside search 25 percent.
- Public areas 25 percent.
- Detailed building search 50 percent.

b. Equipment:

- Specialized.
- Available.

c. Evacuation Procedures (threat received and bomb found)

- (1) Predesignated routes of evacuation.
- (2) Priorities for people removal.
- (3) Predesignated guides.
- (4) Other considerations:
 - Authority to order evacuation.
 - Decision to permit reentry into building.
 - The signal to evacuate.
 - Who will be the evacuation team.
 - What are the evacuation procedures.
 - Destination of evacuation occupants.
 - Responsibilities of the occupants during evacuation.

5. Telephonic Threat Complaint. Figure A is OPNAV 5527/8 which is the approved form for recording telephonic bomb threats. This form is available through supply channels and is issued in pads of 25.

DEPARTMENT OF THE NAVY

TELEPHONIC THREAT COMPLAINT

IF BOMB THREAT, ASK THE

- WHEN IS THE BOMB TO GO OFF
- WHERE IS THE BOMB TO GO OFF
- WHAT KIND OF BOMB IS IT?
- WHAT DOES THE BOMB LOOK LIKE
- WHERE ARE YOU CALLING FROM

1. COMMAND

a. Name & Address

b. Phone No.

2. COMPLAINANT

a. Name

3. PERSON RECEIVING CALL

a. Name

b. Date & Place of Birth

c. Command Name & Address

d. Phone Number
(Work)

(Home)

4. TELEPHONE CALL RECEIVED ON

a. Phone Number (Include area code)

b. Location

c. Phone number listed in ("x" all that apply)

☐

Command Directory

☐

Base Directory

☐

Local Directory

☐

Unlisted

☐

Other (list)

5. DETAILS OF CALL

a. Date

b. Day of Week

c. Time

6. CONTEXT OF CONVERSATION

a. Recipient "

b. Caller "

c. Recipient "

d. Caller "

e. Recipient "

f. Caller "

7. BACKGROUND NOISES (Describe street sounds, voices, music, etc. If more space is needed, continue on reverse.)

8. INFORMATION ABOUT CALLER/VOICE CHARACTERISTICS

a. Sex

b. Age

c. Race

d. Accent

e. Educational Level

f. Attitude (Calm, Nervous, Serious)

g. Other

9. WERE THERE ANY
WITNESSES TO THE CALL?☐ No☐

Yes (List name)

10. DO YOU HAVE ANY SUSPICION AS
TO THE IDENTITY OF THE CALLER?☐ No☐

Yes (List name)

11. NOTIFICATION OF AUTHORITY ("X" all notified)

☐☐☐☐ Security☐ NISRA☐ Telephone Company☐ EOD☐ Fire Dept

APPENDIX IV

PILFERAGE/LARCENY AND ITS PREVENTION

1. Pilferage

a. In this appendix, pilferage refers to the theft of U. S. government property. Pilferage is probably the most common and annoying hazard with which security personnel are concerned. It can become such a financial burden and detriment to operations that a large portion of the security force efforts may have to be devoted to its control. Pilferage, particularly petty pilferage, is frequently difficult to detect, hard to prove, and dangerous to ignore.

b. It is imperative that all naval personnel, civilian and uniformed, to include the management, understand the potential losses to the Navy on a daily basis.

c. Yearly, naval installation property loss throughout the world would increase millions of dollars each year if subjected to undeterred pilferage. However, the risks incurred cannot be measured in terms of dollars alone. Loss of critical supplies for operational units could result in unnecessary loss of life and danger to national defense. In some areas, losses could assume such proportions as to jeopardize the mission of the activity. All activities can anticipate loss from pilferage. Actual losses will depend on such variable factors as type and amount of materials, equipment, and supplies produced, processed, and stored at the activity; numbers of persons employed; social and economic conditions in surrounding communities; command attitudes (this is a most important consideration); and physical security measures employed. Because these factors differ greatly in various types of activities and in different geographical locations, each must be considered separately.

d. To determine the severity of this hazard at any given installation or facility, there is a need to determine the amount of loss which may be occurring. Unfortunately, this is not always an easy task. Accounting methods may not be designed to pinpoint thefts; consequently, such losses remain undisclosed or they are lumped together with other shrinkages, thus effectively camouflaging them.

e. One of the most common inventory methods is to conduct periodic inventories of property and assume that unaccounted for inventory loss is due to theft. This is a convenient but deceptive procedure, because theft is only one of many causes of inventory shrinkage.

16 SEP 1985

f. Failure to detect shortages in incoming shipments, improper stock usage, poor stock accounting, poor warehousing, improper handling and recording of defective and damaged stock, and inaccurate inventories cause inventory losses that may be inaccurately labelled as pilferage.

g. In some cases inventory losses may be impossible to detect because of the nature and quantities of materials involved. Stock inventory records may not be locally maintained, or there may be no method for spot checks or running inventories to discover shortages.

(1) This is an undesirable situation and should be corrected where possible. Recommendations should be made that running inventories be maintained.

(2) An established estimate of the degree of severity of this hazard may have to be revised because of anticipated changes in the economic or social conditions in nearby communities, increases in numbers of employees, introduction of new materials into the activity, or any of the other factors on which estimates of expected losses are based.

(3) The degree of risk involved can be determined only by analysis of the relative vulnerability of each area or activity of the installation to the hazard of pilferage. To do this, it is necessary to consider the problem of who is likely to steal, and what items they are most likely to take.

2. Profile of Pilferers. There are two types of pilferers who physical security personnel must be prepared to counteract - or at least recognize so proper physical security measures may be taken to afford the best protection against them. These are casual pilferers and systematic pilferers.

a. A casual pilferer is one who steals primarily because he is unable to resist the temptation of an unexpected opportunity and has little fear of detection. There is usually little or no planning or premeditation involved in casual pilferage and the pilferer normally acts alone. He may take items for which he has no immediate need or foreseeable use, or he may take small quantities of supplies for use of family and friends, or for use around his home. The degree of risk involved in casual pilferage is normally slight unless very large numbers of persons are involved.

(1) Casual pilferage occurs whenever the individual feels the need or desire for a certain article and the opportunity to take it is provided by poor security measures. Though it involves unsystematic theft of small articles, casual

16 SEP 1985

pilferage is nevertheless very serious, and it may have a great cumulative effect if permitted to become widespread - especially if the stolen items have a high cost or potential value.

(2) There is always the possibility that casual pilferers, encouraged by successful theft (track record) may turn to systematic pilferage. Casual pilferers are normally employees of the installation and usually are the most difficult to detect and apprehend.

b. A systematic pilferer is one who steals according to preconceived plans, and steals any and all types of supplies to sell for cash or to barter for other valuable or desirable commodities.

(1) He may work with another person or with a well-organized group of people, some of whom may be members of a cleaning team or even be in an advantageous position to locate or administratively control desired items, or remove them from storage areas or transit facilities.

(2) The act of pilferage may be a one-time occurrence, or such acts may extend over a period of months or even years. Large quantities of supplies, with great value, may be lost to groups of persons engaged in elaborately planned and carefully executed systematic pilferage activities.

(3) Systematic pilferers may or may not be employees of the installation; if they are not, they frequently operate in conspiracy with such employees.

3. Motivation of Pilferers. The degree of dishonesty may vary with the motivation of pilferers. The uses pilferers make of pilfered items and/or the money from them does not establish any patterns. In fact, their modus operandi is difficult to detect due to their changing motivational desires.

a. The military or civilian thief may:

(1) Not be profit oriented.

(2) Be any person.

(3) Operate with others.

b. Usually, the common danger signs that a pilferer is at work are:

16 SEP 1985

(1) Increase in personal financial spending.

(2) Refusal to accept office, activity or installation movement control procedures.

c. A pilferer's rationalization to dishonesty is:

(1) "Why not, others are doing it."

(2) "It's morally right to me."

(3) "It's not stealing, only borrowing."

d. Elements that induce dishonesty:

(1) Target of opportunity.

(2) High personal need or desire.

(3) Rationalization of personal actions.

4. Targets for Pilferage. Both the casual and systematic pilferers have certain problems to overcome in order to accomplish pilferage objectives. Some of these are:

a. A pilferer's first requirement is to locate the item or items to be stolen.

b. The second requirement is to determine the manner in which he can gain access to and possession of the desired items.

c. The third requirement is to remove the stolen items to a place where the thief may benefit from his act.

d. Finally, to derive any benefit from his act, the pilferer must use the item himself or dispose of it in some way. The casual pilferage of supplies is intended primarily to satisfy the need or desires of the thief. The systematic pilferer usually attempts to sell the material through "fences", pawnbrokers, or black market operations.

5. Methods of Pilferage. There are many ways by which pilfered items may be removed from military installations. Because the motives and targets likely to be selected by systematic and casual pilferers are very different, the methods of operation for each are very different.

a. As stated, the casual pilferer steals whatever is available to him and generally removes it from the installation by concealing it on his person or in his automobile.

b. The methods of the systematic pilferer are much more varied and complex. The means he may employ are limited only by his ingenuity. The following are cited examples:

(1) Shipping and receiving operations are extremely vulnerable to systematic pilferage. It is here that installation personnel and truck drivers have direct contact with each other and readily available means of conveyance.

(2) One individual must not have control of all shipping and receiving transactions. The opportunities for monetary kickbacks increase without a sound system of checks and balances.

(3) Railway employees assigned to switching duties on the installation can operate in a similar manner but with more difficulty because a railway car normally cannot be directed to a location where stolen property can be easily and safely removed.

(4) Tanker trucks employed for shipment of petroleum products may be altered to permit pilferage of the product.

(5) Trash disposal and salvage disposal activities offer excellent opportunities to the systematic pilferer to gain access to valuable material. Property may be hidden in waste material to be recovered by a confederate who removes trash from the activity.

6. Control Measures for Pilferage. Specific measures for preventing pilferage must be based on careful analysis of the conditions at each installation. The most practical and effective method for controlling casual and systematic pilferage is to establish psychological deterrents. This may be accomplished in a number of ways.

a. One of the most common means of discouraging casual pilferage is to inspect individuals and vehicles leaving the installation at unannounced times and places. Gate inspection procedures involve legal restrictions emanating from the Fourth Amendment to the U. S. Constitution. These procedures must comport with judicially acceptable standards, including a bona fide method of random selection of vehicles stopped for inspection. Liaison with the cognizant staff judge advocate is required prior to instituting such procedures.

b. An aggressive security education program is an effective means of convincing employees that they have much more to lose than to gain by engaging in acts of theft.

16 SEP 1985

c. It is particularly important for supervisory personnel to set a proper example and maintain a desirable moral climate for all employees.

d. All employees must be impressed with the fact that they have a responsibility to report any loss to proper authorities.

e. Adequate inventory and control measures should be instituted to account for all material, supplies, and equipment.

f. Identification of all tools and equipment by some mark or code (where feasible) is necessary so that government property can be identifiable. Another control method is to require signing for all tools and equipment to be used by individuals. The use of the signature control method reduces the temptation to pocket the item.

g. In establishing any deterrent to pilferage, physical security officers must not lose sight of the fact that most employees are honest and disapprove of thievery. Any security measure that infringes on the human rights or dignity of others will jeopardize, rather than enhance the overall protection of the installation.

h. Other measures that should be considered to eliminate losses attributed to the systematic pilferer include:

(1) Establish security surveillance of all exits from the activity.

(2) Establish an effective package and material control system.

(3) Locate parking areas for private vehicles outside the perimeter fencing of the activity.

(4) Eliminate potential thieves during the hiring procedure by careful screening and observation.

(5) Investigate all losses quickly and efficiently.

(6) Establish an effective key control system.

(7) Install mechanical and electrical intrusion detection devices where applicable and practical.

(8) Coordinate with supply personnel to establish customer identification, to authenticate supply release documents at warehouses and exit gates.

(9) Establish appropriate perimeter fencing, lighting and parking facilities and effective pedestrian, railway, and vehicle gate security controls.

i. Small items of equipment, tools and supplies which are easily pilferable must be stored in a caged area or equivalentlly secured. Access to the area must be limited to employees authorized entrance by duty position. A running inventory should be maintained and checked by supervisory personnel on a periodic basis.

7. Employee Theft. No matter what it's called - internal theft, peculation, embezzlement, pilferage, inventory shrinkage stealing, or defalcation - thefts committed by employees are behind at least 60 percent of crime-related losses. So many employees are stealing so much that employee theft is the most critical crime problem facing business today. Although employee theft results in part from factors beyond control, the extent of employee theft in any business is a reflection of its management - the more mismanagement, the more theft.

a. An effective stop-employee-thefts policy must include at least the following:

- (1) Preemployment screening.
- (2) Analysis of opportunities for theft.
- (3) Analysis of how employees steal.
- (4) Management - employee communication.
- (5) Prosecution of employees caught stealing.

b. Each employer must reduce losses as much as possible. A police state need not be created. Large monetary expenditures need not be made.

8. Loss Prevention. Too many opportunities exist for employees to exploit. Reduce these opportunities through a comprehensive and viable loss prevention program and losses will be reduced.

16 SEP 1985

APPENDIX V

LEGISLATIVE JURISDICTION
AND THE AUTHORITY OF SECURITY PERSONNEL

1. Scope. This appendix defines and discusses the different types of legislative jurisdiction; it outlines the advantages and disadvantages that each type of jurisdiction has with respect to the physical security function. Finally, this appendix briefly outlines the authority of security personnel act in response to suspected on-base offenses (particularly offenses committed by civilians).

2. "Jurisdiction" Defined. As used in this appendix, jurisdiction refers to the authority to legislate general, municipal law in a given area. This authority derives from a specific constitutional provision (U. S. Const., art. I, 8, c. 17).

a. Legislative jurisdiction must be distinguished from the general legislative authority of Congress which is not dependent on land area, but upon subject matter or purpose; e.g., Internal Revenue Code, VA Benefits, Immigration, etc.

3. Types and Degree of Jurisdiction. In a 1956 U. S. Attorney General report entitled "Report of the Interdepartmental Committee for the Study of Jurisdiction over Federal Areas Within the States, pt. 1 (1956)", the four degrees of jurisdiction were defined with advantages and disadvantages of each, as follows:

a. Exclusive Legislative Jurisdiction, which applies to situations wherein the Federal Government has received, by whatever method, all the legislative authority of the State, with no reservation made to the State except of the right to serve process resulting from activities which occurred off the land involved. This shall be referred to as exclusive federal jurisdiction.

(1) Advantages

(a) Activity commanding officer has full control of law enforcement to the exclusion of state and local authorities.

(b) The State cannot enforce its municipal laws on a tract of Federal land which falls under this jurisdiction. Federal authorities, however, can prosecute State criminal offenses which are committed on Federal land pursuant to the Assimilative Crimes Act (18 U.S.C. 13).

(NOTE: Two federal forums are available: U. S. magistrates' court and U. S. district court. Generally, U. S. magistrates try only minor offenses such as traffic violations [reference (h)]. The cognizant Assistant U. S. Attorney may, in his/her discretion, not prosecute minor offenses such as simple assault. Person suspected of committing a felony may be tried in U. S. district court.)

(2) Disadvantages

(a) Criminal offenses committed in areas of exclusive federal jurisdiction cannot be investigated by state law enforcement authorities nor prosecuted in state courts.

(b) DoD security force personnel do not possess general statutory police powers. Their authority stems from the inherent authority of the federal government to protect its property and functions, and from citizens' arrest principles which vary from state to state.

(c) DoD security force personnel cannot rely upon assistance from state law enforcement agencies in areas of exclusive federal jurisdiction. State laws, including statutory police powers, do not apply in areas of exclusive federal jurisdiction. On-base personnel may be turned over to civilian authorities pursuant to Chapter XIII of the Navy Manual of the JAG.

(NOTE: A State Trooper in fresh pursuit, for example, may enter the Federal land, accompanied by a DOD officer, and continue pursuit. Apprehension however, would be made by the DOD officer and the offender would be turned over to the State Trooper at the gate (boundary) of the Federal land.)

b. Concurrent Legislative Jurisdiction which applies in those instances where in granting to the United States authority which would otherwise amount to exclusive legislative jurisdiction over an area, the State has reserved to itself the right to exercise, concurrently with the United States, all of the same authority. This shall be referred to as concurrent jurisdiction.

(1) Advantages

(a) Both state and federal general municipal laws are applicable.

(b) The government has the option of prosecuting an offense through either the State or Federal judicial systems.

(c) DoD civilian security forces can be deputized by the State. As State Peace Officers the DoD police can enforce state statutes on Federal land. Generally, deputization is not necessary since DoD personnel may, under U. S. Navy Regulations, 1973, art. 0713, investigate, detain, and deliver to civil authorities, civilians who are suspected of criminal wrong doing.

(d) When state law enforcement authorities enter Federal property they retain their State Statutory police powers.

(NOTE: Thus, state police may (subject to the commanding officer's approval) enter a military installation and apprehend an offender without the assistance or presence of DoD security force personnel.)

(2) Disadvantages. Activity commanding officers share legislative jurisdiction with the state (regulatory powers of the state may be exercised, but not so as to interfere with federal functions).

(NOTE: States may not control federal operations, nor may they impair or destroy the effective use of property by the United States.)

c. Partial Legislative Jurisdiction, which applies in those instances wherein the Federal government has been granted to exercise by it over an area in a State certain of the State's authority, but where the State concerned reserved to itself the right to exercise, by itself or concurrently with the United States, other authority more than the right to serve civil or criminal process in the area (e.g., the right to tax private property). This shall be referred to as partial jurisdiction.

(1) The advantages/disadvantages related to this type of authority vary with the circumstances of each individual activity or tract of land. The key factor concerns the specific authority the State has retained to exercise by itself or concurrently with the United States.

d. Proprietorial Interest Only, which applies in those instances when the federal government has acquired some right or title to an area in the state but has not obtained any measure of the state's authority over the area (this does not preclude the federal government from exercising its other constitutional powers; e.g., protection of government property). This shall be referred to as proprietorial jurisdiction. In these areas, prosecution for non-federal, minor offenses will occur in state courts only.

16 SEP 1985

(1) Advantage. If civilian law enforcement agencies are willing and able to provide police services, there may be less need for DoD security resources. However, enforcement of the UCMJ will remain primarily a military function.

(2) Disadvantage. Commanding officers may have less control of law enforcement in these areas since there may be a greater reliance on civilian law enforcement agencies.

4. Authority of Security/Law Enforcement Personnel

a. Authority over civilians. Some federal law enforcement personnel have statutory police powers provided by federal law. DoD guard personnel have no such authority. The authority of DoD guards to maintain the security of government property and employees stems from the inherent authority of the federal government to protect the viability of its constitutional functions. This is reflected in U. S. Navy Regulations, 1973. These regulations reflect the absolute responsibility of the commanding officer for his command (art. 0702); the specific responsibility to maintain security (art. 0736); the responsibility to control and supervise visitors (art. 0714); and the authority to surveil, investigate, detain, and deliver to civilian authorities non-military personnel present on a military installation under incriminating or irregular circumstances (art. 0713). In addition, civilians may be barred from re-entry onto the installation (18 U.S.C. 1382).

b. Guard personnel may also act in furtherance of their personal civil authority; that is, their authority to make a citizen's arrest. This raises the issue of state legislative jurisdiction: In areas where the United States does not have exclusive federal jurisdiction, citizen's arrest is defined by the laws of the state. In areas of exclusive federal jurisdiction, the common law rule has been applied. The common law provides that a private citizen may arrest, without a warrant: (1) a person whom he knows to have committed a felony; (2) one whom he reasonably and in good faith believes has committed a felony, where a felony has in fact been committed; (3) one whom he finds committing or attempting to commit a felony; or (4) a person committing a misdemeanor in his presence if the misdemeanor involves a breach of the peace.

c. Authority over military personnel. Civilian guard personnel may, upon probable cause, apprehend military personnel for offenses cognizable under the UCMJ (R.C.M. 203(b); 10 U.S.C. 807).

APPENDIX VI

PHYSICAL SECURITY AND THE POSSE COMITATUS ACT

1. This iteration of the physical security instruction deletes reference to law enforcement in order to provide separate treatment to the commanding officer's function of providing physical security. A commanding officer has different constraints in areas of law enforcement than in the performance of other Federal functions.
2. The legal constraint which affects the law enforcement function, and which could in turn affect the physical security function is embodied in the Posse Comitatus Act, (18 U.S.C. 1385) which provides; "[w]hoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws shall be fined not more than \$10,000 or imprisoned not more than two years or both." Although not expressly applicable to the Navy or Marine Corps, the Posse Comitatus Act is applicable to the DoN as a matter of policy [reference (t)]. However, the posse comitatus limitation does not restrict activity which is primarily in furtherance of a military purpose, even if such activity yields incidental benefits to civilian law enforcement officials.
3. Physical security of military personnel and military property clearly entails a military function and purpose; thus activity in furtherance of physical security will generally not be affected by the constraints of the Posse Comitatus Act. Law enforcement activity; e.g., the investigation of suspected criminal activity; is more likely to involve posse comitatus constraints, especially when civilians are the subject of the investigation or when the investigation is of the type normally handled by civilian (non-DoD) law enforcement agencies. Accordingly, security personnel should keep in mind that their mission (as defined in this instruction) is normally not constrained by the Posse Comitatus Act so long as their actions remain primarily in furtherance of protecting DoD personnel and property. Questions regarding the propriety of any activity in light of the Posse Comitatus Act shall be referred to the cognizant staff judge advocate for advice.

16 SEP 1985

APPENDIX VII

CLASSIFICATION

Activity:

Date:

PHYSICAL SECURITY PLAN

1. Purpose. State purpose of the plan.
2. Area Security. Define the areas, buildings, and other structures considered critical and establish priorities for their protection.
3. Control Measures. Define and establish restrictions on access and movement into critical areas. These restrictions can be categorized as to personnel, vehicles, and materials.

a. Personnel Access:

- (1) Establish controls pertinent to each area or structure.

- (a) Authority for access.

- (b) Access criteria for:

- 1 Assigned personnel.

- 2 Visitors.

- 3 Maintenance personnel.

- 4 Contractor personnel.

- (2) Identification and control

- (a) Describe the system to be used in each area. If a badge system is used, a complete description covering all aspects should be used in disseminating requirements for identification and control of personnel conducting business on the installation.

CLASSIFICATION

16 SEP 1985

CLASSIFICATION

(b) Application of the system.

1 Assigned personnel.

2 Visitors to restricted areas.

3 Visitors to non-restricted areas.

4 Vendors, tradesmen, etc.

5 Contractor personnel.

6 Maintenance or support personnel.

b. Material Control

(1) Incoming

(a) Requirements for admission of material and supplies.

(b) Search and inspection of material for possible sabotage/terrorist hazards.

(c) Special controls on delivery of supplies and/or personnel shipments in restricted areas.

(2) Outgoing

(a) Documentation required.

(b) Controls, as outlined in (1) (a), (b), and (c) above.

(c) Classified shipments NOT involving hazardous material.

(3) Hazardous material (OPNAVINST 3710.31)

(a) Controls on movement of hazardous material on the installation.

(b) Controls on shipments or movement of hazardous material outside the installation.

CLASSIFICATION

CLASSIFICATION

c. Vehicle Control

(1) Policy on administrative inspection of military and privately owned vehicles.

(2) Parking regulations.

(3) Controls for entrance into restricted and non-restricted areas.

(a) Privately owned vehicles.

(b) Military vehicles.

(c) Emergency vehicles.

d. Vehicle Registration

4. Aids to security. Indicate the manner in which the following listed aids to security are to be implemented on the installation.

a. Protective barriers

(1) Definition.

(2) Clear zones.

(a) Criteria.

(b) Maintenance.

(3) Signs

(a) Types.

(b) Posting.

(4) Gates

(a) Types.

(b) Posting.

(c) Lock security.

CLASSIFICATION

CLASSIFICATION

b. Protective Lighting Systems

- (1) Use and control.
- (2) Inspection.
- (3) Action to be taken in the event of commercial power failure.
- (4) Action to be taken in the event of a failure of alternate source of power.
- (5) Emergency lighting systems.
 - (a) Stationary.
 - (b) Portable.

c. Intrusion Detection Systems

- (1) Security classification.
- (2) Inspection.
- (3) Use and monitoring.
- (4) Action to be taken in event of "Alarm" conditions.
- (5) Maintenance.
- (6) Alarm logs or registers.
- (7) Sensitivity settings.
- (8) Fail-safe and tamper-proof provisions.
- (9) Monitor panel location.

d. Communications

- (1) Locations.
- (2) Use.
- (3) Tests.
- (4) Authentication.

16 SEP 1985

CLASSIFICATION

5. Security Forces. Include general instructions that apply all security force personnel (fixed and mobile). Detailed instructions such as Special Orders and SOP should be highlighted.

- a. Composition and organization.
- b. Tour of duty.
- c. Essential posts and routes.
- d. Weapons and equipment.
- e. Training.
- f. Use of sentry/patrol dogs.
- g. Method of challenging.
- h. Crisis response force.
 - (1) Composition.
 - (2) Mission.
 - (3) Weapons and equipment.
 - (4) Location.
 - (5) Deployment concept.

6. THREATCONS/Crisis Management. Indicate required actions response to various emergency situations.

7. Coordinating Instructions. Indicate matters which require coordination with other military and civil agencies.

CLASSIFICATION

16 SEP 1985

CLASSIFICATION

a. Integration with plans of host, tenant or nearby military installations.

b. Liaison and coordination.

(1) Local civil authorities.

(2) Federal agencies.

(3) Military organizations.

/s/ _____
Commanding Officer

Annexes: (as appropriate)

A - Intelligence (threat assessment)

B - Installation Security Status Map (including legislative jurisdiction)

CLASSIFICATION

APPENDIX VIII

PHYSICAL SECURITY SURVEY CHECKLIST

The purpose of this checklist is to provide activity security department and management personnel with guidelines for evaluating adequacy of overall security programs. This checklist is not intended to be all inclusive. It is most appropriate for larger activities, but many questions are relevant at smaller installations and activities.

UNIT/ACTIVITY BEING SURVEYED:

UIC: _____

Each activity shall conduct physical security self-surveys at least annually. Activities will maintain physical security surveys and make them available to Inspectors General during Command inspections of their respective activities.

1. Answer each question with a "yes", "no", or "N/A", as appropriate.
2. If a requirement is applicable but a waiver or exception has been approved or requested, check the "N/A" column and make reference to the approving authority or requesting document, including the waiver or exception number.
3. Some questions are asked for documented information only and are not requirements or standards. These questions normally do not bear a reference, but shall be answered and data provided, as requested.

CHAPTER 1

INTRODUCTION

	YES	NO	N/A	REF
1. Is a security officer designated in writing?				0111b
2. Is the designated security officer at least a GS-11 or above, a military officer or senior enlisted, E7/8/9?				0111a
3. Is the security manager designated in writing?				OPNAVINST 5510.1G
4. Has a Physical Security Review Committee (PSRC) been established?				0115
5. Is the PSRC composed of individuals discussed in Chapter 1 of this instruction?				0115b
6. Does the PSRC meet at least quarterly?				0115d
7. Are formal minutes recorded and available for review?				0115d
8. Has a Loss Prevention Subcommittee (LPS) been established?				0115e
9. Does the LPS meet at least monthly?				0115e
10. Are formal minutes recorded and appended to the PSRC quarterly minutes?				0115e
11. Has a Physical Security Review Board (PSRB) been established?				0115f
12. Does the PSRB meet at least semi-annually?				0115f
13. Is the PSRB membership as outlined in paragraph 0115?				0115f
14. Is the security officer included in all initial construction review processes?				0117

16 SEP 1985

CHAPTER 2
SECURITY PLANNING

YES NO N/A REF

1. Does the activity/installation have a current physical security plan (PSP)?

0200

Date of plan_____

2. Does the PSP contain those annexes as outlined in paragraph 0200 of this instruction?

0200

3. Does the PSP contain tenant command Physical Security Plans?

0200

4. If a host command, is physical security planning coordinated with pertinent tenant commands?

0200

5. If a tenant command, is physical security planning coordinated with host command?

0200

6. Does the PSP include:

- a. Preventive measures to reduce opportunities for introduction of bombs?
- b. Procedures for evaluating and handling bomb threats?
- c. Policy for evacuation and safety of personnel?
- d. Procedures to be used to search for bombs?
- e. Procedures in the event a bomb or suspected bomb is found on the premises?
- f. Procedures for obtaining assistance and support of law enforcement and explosive ordnance disposal units?
- g. Procedures to be taken in the event of a bomb explosion or detonation?

7. Does the activity have a countersabotage program?

0208
App I

16 SEP 1985

YES NO N/A REF

8. Does the security officer ensure that physical security surveys are conducted at least annually?

0213

9. How often does the activity commander request a threat assessment from the Naval Investigative Service?

0213c

CHAPTER 3

SECURITY MEASURES

- | | YES | NO | N/A | REF |
|---|-----|----|-----|----------------------|
| 1. Does the activity have a comprehensive Loss Prevention Program? | | | | 0303 |
| 2. Does the activity have a comprehensive Missing, Lost, Stolen, or Recovered (MLSR) program? | | | | 0304 |
| 3. Do all activity/installation departments/offices fully participate in the MLSR reporting program and submit all known MLSR reportable government property? | | | | 0304 |
| 4. How many MLSR incident reports have been submitted thus far this calendar year?_____ | | | | |
| 5. What is the date of the activity's most recent risk and threat analysis? _____ | | | | 0305 |
| 6. Have areas been designated in writing by the commanding officer as exclusive, limited, or controlled, as necessary? | | | | 0306a |
| 7. Are the basic security measures for exclusion areas listed in Chapter 3 in effect? | | | | 0306c(1) |
| 8. Are the basic security measures for limited area listed in Chapter 3 in effect? | | | | 0306c(2) |
| 9. Are the basic security measures for controlled areas listed in Chapter 3 in effect? | | | | 0306c(3) |
| 10. Are all restricted area points of ingress appropriately posted as prescribed in Chapter 3 of this instruction? | | | | 0307 |
| 11. Are security measures in effect to protect: | | | | |
| a. Electric power supplies and transmission facilities? | | | | |
| b. Communication centers/equipment? | | | | |
| c. Arms, ammunition and explosives? | | | | OPNAVINST
5530.13 |
| 12. Has a key control officer been appointed and designated in writing by the commanding officer? | | | | 0308a |

16 SEP 1985

YES NO N/A REF

13. Have adequate key custodians been appointed in writing? 0308b
14. Has the activity established a central key room? 0308c
15. Are all padlocks to and within restricted areas rotated at least annually? 0308d
16. Does the key and lock control program include:
 - a. A key control register? 0308
 - b. An annual inventory of all keys issued by the key custodian? 0308a
 - c. A system with records showing positive key and lock accountability? 0308f
17. Is the procurement of all security locks and padlocks approved by the security officer? 0308i
18. Do all security containers, vaults and strongrooms conform to standards as outlined in OPNAVINST 5510.1G? 0309
19. Are Physical Security Surveys of the activity conducted at least annually under the auspices of the security officer? 0310
20. What is the date of the most recent physical security inspection, audit, or review by an immediate superior in command?_____ 0310
21. Does the activity have an effective after-hours/weekends restricted area security check by the security force? 0311
 - Are results of security checks promptly reported to the activity security officer? 0311
22. Does the activity have a comprehensive POV parking plan including:
 - a. Restriction of POV parking in exclusion/limited areas? 0312

YES NO N/A REF

- b. Fenced/enclave parking in controlled areas? 0312b
- c. POV parking restrictions as outlined in paragraph 0312 of this instruction? 0312
23. Does the activity have a traffic control program? 0313
24. Are parking areas within controlled areas fenced so that occupants of automobiles must pass through a pedestrian gate when entering or leaving the working area ? 0312
25. Are parking areas within controlled areas located away from sensitive points and perimeter security fencing? 0312
26. Are appropriate signs setting forth the provisions of entry conspicuously posted at all entrances? 0307
27. Are appropriate warning signs posted on or adjacent to installation and restricted area perimeter barriers at 100 foot intervals? 0306c
28. Do all sensitive inventory items, drugs, drug abuse items and precious metals receive adequate security controls as outlined in Chapter 3 of this instruction? 0314
thru
0317

CHAPTER 4

THE SECURITY FORCE

	YES	NO	N/A	REF
1. Is the present security force strength and composition commensurate with the degree of security protection required?				0405
2. Are all security posts, fixed and mobile, provided with security force orders?				0407
3. Are security force orders reviewed by the security officer for currency at least monthly?				0407c
4. Do security force members have security clearances equivalent to the highest degree of security classification of the documents, material, etc., to which access may be required?				0408
5. Do civil service members of the security force meet the minimum qualifications of the Office of Personnel Management qualification standards?				0409b
6. If a composite security force is used, are there separate supervising echelons for military and civilian elements?				0409c
7. Are security force personnel inspected and briefed by a supervisor prior to being posted?				0409e
8. Do supervisors inspect each post/patrol/ activity at least twice per shift?				0409e
9. Does the activity maintain an organized and equipped Crisis Response Force?				0418
10. Does the Crisis Response Force receive adequate training?				0418e
11. How many military personnel are available who could be utilized by the host command to support the civilian security force in any emergency?				0418d

On station_____

YES NO N/A REF

Off station, with a statement of how many could be recalled to reach the station in:

- a. one hour notice_____
 - b. four hour notice_____
 - c. any pertinent comments:_____
-

12. Are there agreements, verbal or written, with nearby Navy, Army, Air Force or Marine Corps installations from which, in the event of riot, disaster, sabotage, etc., assistance would be provided (For host commands only.).

Name of installation:_____

Distance (in miles):_____Travel time:_____

Type of agreement (verbal/written, ISSA, etc.)

Brief description:_____

13. In the event no written/verbal agreements exist, is there a military installation nearby with sufficient personnel to warrant exploring the feasibility of establishing such an agreement? (For host commands only.)

Name of installation:_____

Distance (in miles)_____ Travel time:_____

14. Has liaison been established with local, state and Federal law enforcement agencies whereby early warning of threat situation will be provided?

0213

15. Are general and special guard orders properly posted?

0407

16. Do security force personnel know their general and special orders?

0409e

YES NO N/A REF

17. Are periodic inspections and examinations conducted to determine the degree of understanding and compliance with all guard general and special orders?

0409e

18. Do security force personnel record or report their presence at key points in the installation by means of:

0409f

- a. portable watch clocks,
- b. central watch clock stations,
- c. telephones
- d. two-way radio communications equipment, or
- e. other?_____

19. Are guard assignments, times and patrol routes varied at frequent intervals to avoid establishing routines?

CHAPTER 5

PERSONNEL AND VEHICLE MOVEMENT CONTROL

YES NO N/A REF

1. Is a pass or badge identification system used to identify all personnel within the confines of restricted areas in effect?

0503

2. Does the identification medium in use comply with Chapter 5 and provide the desired degree of security?

3. Do written instructions include arrangements for the following:

a. Protection of coded or printed components of passes and badges?

0506b

b. Retrieval and safeguarding printer's plates for passes and badges?

0504a

c. Controlled issue of identification media?

0503/0504

d. Providing lost badge listings to all security posts?

0506c

e. Description of the various identification media involved and the authorization and limitation placed upon the bearer?

0504

f. Mechanics of identification upon entering and leaving each area, as applied to both employees and visitors?

0502/0505

g. Details of where, when and how badges shall be worn?

0503d

h. Procedures to be followed in case of loss or damage to identification media?

0506b

i. Procedures for recovery and revalidation?

0505/
0506b

j. Accounting for each badge and pass?

0504a

16 SEP 1985

YES NO N/A REF

4. If a badge exchange system is used for any restricted area, does the system provide for:

- | | |
|---|-------|
| a. Comparison of badges, passes and personnel? | 0506 |
| b. Physical exchange of pass/badge at time of entrance/exit? | 0506 |
| c. Location and verification of personnel remaining within restricted areas at the end of normal working hours? | 0505a |

5. Are personnel who require infrequent access to a restricted area or who have not been issued a permanent pass or badge for such, treated as "visitors" thereto and issued a visitors' badge or pass?

0505b

6. Do guards at control points compare badges to bearers, both upon entry and exit?

0506

If no, upon entry only?

Upon exit only?

7. Is supervision of the personnel identification and control system adequate at all levels?

0506

8. Are badges and serial numbers recorded and controlled by rigid accountability procedures?

0504

9. Are lost badges replaced with badges bearing different serial numbers?

0506b

10. Have procedures been established that provide for issuance of temporary badges for individuals who have forgotten their permanent badges?

11. Are all contractors performing work in restricted areas issued special and distinct contractor badges?

0505c

Are they required to wear the badges at all times exposed, while performing work in restricted areas?

12. Are temporary badges used?

YES NO N/A REF

13. Are badges of such design and appearance as to enable guards and other personnel to recognize quickly and positively the authorizations and limitations applicable to the bearer? 050

14. Are procedures in existence to ensure the return of identification badges upon termination of employment or assignment? 0504
050

15. Have effective visitor escort procedures been established? 0502

16. Are visitors properly escorted within restricted areas?

17. Are procedures established to ensure against the use of the U.S. Government Identification Card (Optional Form 55) being used to gain entry into restricted areas? 0502

18. What controls are employed to control visitor movements while in restricted areas? 050

19. Are visitors required to conspicuously display identification media on outer garments, in front, above the waist at all times while within restricted areas?

20. Are permanent records of visits maintained? 050

a. By whom? _____

21. What measures are employed, other than issuance of identification badges, to control the movement of contractor personnel working within restricted areas?

_____.

YES NO N/A REF

22. Are privately owned vehicles (POV) and contractor vehicles which are allowed routine access to the installation registered with the security office?

0509

23. Have written procedures been issued for the registration of POV's authorized aboard the installation?

0509a

24. Are random administrative inspections made of automobiles?

0509f

a. Are procedures issued by the commanding officer and are they concise and specific?

25. Does the activity use the standard DOD decalcomania system for registration of POVs and other eligible vehicles?

0509a

26. Are procedures in effect requiring the checking of government vehicle trip tickets for off-station authorization by security force personnel?

CHAPTER 6

BARRIERS AND OPENINGS

YES NO N/A REF

1. Does the fenced portion of the restricted area barrier meet the minimum specifications for security fencing? 0603
- a. Is it of chain link (cyclone) composition? 0603a
- b. Is it constructed of 9-gauge or heavier wire? 0603a
- c. Is the mesh opening no larger than two inches? 0603a
- d. Is selvage twisted and barbed at top and bottom? 0603a
- e. Is the bottom of the fence within two inches of solid ground? 0603a
- (1) In areas where the fence exceeds two inches from solid ground, have compensatory measures been taken?
- f. Is the top guard strung with barbed wire (or barbed tape/razor edge) and angled outward away from protected site and upward at a 45 degree angle? 0603a
- g. Is the fence at least 8 feet in height (including outrigger) in all required areas? 0603a
2. Does the activity provide for security force inspection of the security barrier, including clear zones, at least once per month? 0608/
0606e
- a. Are deficiencies noted and are remedial actions promptly effected?
3. If masonry wall is used, does it meet minimum specifications for security fencing? 0604
4. If building walls, floors and roofs form a part of the barrier, do they provide security equivalent to that provided by a chain link fence? 0604

16 SEP 1985

YES NO N/A REF

5. Are all openings properly secured? 0603

6. If a building forms a part of the barrier, does it present a potential penetration hazard at the point of juncture with the perimeter security fence? 0603

7. If a body of water forms any part of the barrier, are additional security measures provided?

8. Are openings such as culverts, tunnels, man-holes for sewers and utility access, and sidewalk elevators which permit access to the installation and restricted area properly secured? 0611
0612
0613

9. Are all portals in perimeter barriers guarded or secured? 0609

10. Do the gates and/or other entrances in perimeter barriers exceed the number required for safe and efficient operation? 0609/
0610

11. Are all perimeter barrier portals equipped with secure locking devices? 0609/
0610

a. Are they locked when not in use? 0610

12. Do all gates provide protection equivalent to that provided by the barrier of which they are a part? 0610

13. Are barrier gates and/or other entrances which are not in active use locked and frequently inspected by guards or other personnel? 0610b

14. Are locks to all gates, active and inactive, rotated at least annually? 0610b

15. Does the security officer provide adequate protection and accountability of keys to security barrier entrances? 0610b

a. If not, specify responsible individual or office. _____

YES NO N/A REF

16. Are keys to barrier entrances issued to other than installation personnel?
17. Are automobiles permitted to park within clear zones? 0312
18. Are prescribed clear zones maintained on both sides of the restricted area barriers? 0606
19. If clear zone requirements cannot be met, have compensatory security measures been implemented? 0606d
 - a. Have waivers or exceptions been obtained or initiated for obstacles within clear zones which are not considered cost effective to relocate?
20. Are lumber, boxes or other extraneous material allowed to be stacked against or adjacent to the barrier? 0606
21. Are adequate interior all-weather security roads provided for the use of security patrol vehicles? 0607
22. If security patrols or other security activities along the perimeter have been changed since the last survey, specify the change:

23. Are any perimeters protected by intrusion detection systems (IDS)?
24. Have any additional barriers been installed or has any relocation thereof been accomplished since the last survey? If so, briefly describe:

OPNAVINST 5530.14A

16 SEP 1985

YES NO N/A REF

25. Does any relocated function, newly designated restricted area, physical expansion, or other factor indicate necessity for installation of additional barriers or additional perimeter lighting? If so, briefly explain what action have been taken or planned.

CHAPTER 7

PROTECTIVE LIGHTING

YES NO N/A REF

1. Is the perimeter of the installation and restricted area fencing provided adequate lighting? 0701a
2. Does the protective lighting meet adequate intensity requirements? (Chapter 5, Section 3 of reference (r)) 0701
3. Are the cones of illumination from lamps directed downward and away from guard personnel? 0701c
4. Is perimeter protective lighting utilized so that security force patrol personnel remain in comparative darkness? 0701c
5. Are lights checked for proper operation prior to darkness at least once daily? 0704
6. Are defective lights and need for replacement of inoperative lamps reported immediately? 0704
7. Are repairs to lights and replacement of inoperative lamps effected immediately or in a reasonable time? 0704
8. Is additional lighting provided at active portals and points of possible intrusion? 0704
(b&c)
9. Are gate guard houses provided with proper illumination? 0704
10. Does the activity have a dependable source of power for its protective lighting system? 070
11. Does the activity have a dependable auxiliary (emergency) source of power for protective lighting? 070
12. Is the protective lighting system independent of the activity lighting or power system? 0706
13. Is the power supply for the protective lighting system protected? 070

a. How is it protected?_____.

16 SEP 1985

YES NO N/A REF

14. Are there provisions for standby or emergency protective lighting? 0705
15. Is the standby or emergency equipment tested at least monthly? 0705
16. Can the emergency backup power supply be rapidly switched into operation when needed? 0704
0705
17. Is the emergency backup power supply self-starting? 0705
18. Is the protective lighting/emergency or standby power source located within a restricted area? 0705
19. Is parallel circuitry used in the wiring? 0706c
20. Are multiple circuits used? 0706c
- a. If yes, are proper switching arrangements provided?
21. Are switches and controls properly located, controlled and protected? 0707
- a. Are they weatherproof and tamper resistant?
- b. Are they readily accessible to security personnel?
- c. Are they located so that they are inaccessible from outside the perimeter barrier?
- d. Is there a centrally located switch to control protective lighting?
22. When was the most recent activity lighting energy conservation opportunities (LECO) study conducted? _____
23. When was the most recent installation/restricted area protective lighting survey conducted? _____
24. Is the protective lighting system designed and locations recorded so that repairs can be made rapidly in an emergency?

YES NO N/A REF

25. Are materials and equipment in shipping and storage areas properly arranged to provide adequate lighting?

07040

26. If bodies of water form a part of the perimeter, is adequate lighting provided where deemed appropriate?

0704

16 SEP 1985

CHAPTER 8

INTRUSION DETECTION SYSTEMS

YES NO N/A REF

1. Does the activity employ any Intrusion Detection Systems (IDS)?

2. Does the IDS, where required or used, meet the following minimum requirements?

- a. Are balanced magnetic switches installed on all perimeter doors? 0809
- b. Are IDS signals monitored at one central point and is the security force response initiated from that point? 0809b
- c. Are all sensor equipment, doors, drawers and removable panels secured with key locks or screws and equipped with tamper switches? 0809f
- d. Have power supplies been protected against overload by fuses or circuit breakers? 0809g
- e. Have power supplies been protected against voltage transients? 0809g
- f. Have safety hazards been identified and controlled to preclude personnel exposure? 0809h
- g. Is the IDS system equipped with high security electronic line supervision? 0809c
- h. Are annunciator, control and display subsystems located in a separate area or closed off from public view? 0807
- i. Are zone numbers assigned to IDS sensor locations instead of building/room numbers? 0807

3. Is the system backed up by adequate security alert teams? 0802k

4. Is the alarm system for active areas or structures placed in access mode during normal working hours? 0809

16 SEP 1985

YES NO N/A REF

- | | |
|---|------|
| 5. Is the system tested prior to activation? | 080 |
| 6. Is the system inspected at least monthly? | 0812 |
| 7. Is the exterior IDS system weatherproof? | 0805 |
| 8. Is there an alternate or independent power source available for use on the system in the event of power failure? | 0809 |
| 9. Is the emergency power source designed to cut in and operate automatically when AC power goes down? | 0809 |
| 10. Is the IDS system properly maintained by trained and properly cleared personnel? | 0812 |
| a. Are maintenance/installation personnel in-house (military/civilian)? | 0812 |
| 11. If contractor personnel install and maintain the system, are they properly cleared? | 0812 |
| 12. Are emergency maintenance personnel designated? | 081 |
| 13. Are frequent tests conducted to determine the adequacy and promptness of response to alarm signals? | |
| 14. Are records kept of all alarm signals received to include time, date, location, action taken and cause for alarm? | 0812 |

16 SEP 1985

CHAPTER 9PART 1EMPLOYEE SECURITY EDUCATION PROGRAM

YES NO N/A REF

1. Does the activity have a current employee security education program addressing physical security matters? 0901
2. Are all newly assigned personnel provided physical security indoctrination? 0901
3. Is formal security education training conducted for all personnel at least annually? 0901
4. Does the security education program provide for crime prevention and loss prevention measures? 0901b
5. Is attendance monitored to ensure all hands receive this training? 0901
 - a. Are individual employee records kept indicating security education received?
6. Are all personnel indoctrinated in security procedures which apply in the performance of their duties? 0901g
7. Does the program cover such topics as:
 - a. Pass and badge system? 0901g
 - b. Dangers of loose talk and operational carelessness? 0901g
 - c. Privately owned vehicle identification and control? 0901g
 - d. Random package and vehicle inspections? 0901g
 - e. Procedures for prompt reporting of security breaches? 0901
 - f. General security topics? 0901g
8. Are procedures formulated requiring participation by key activity personnel? 0901i

16 SEP 1985

YES NO N/A REF

9. Are local law enforcement agencies asked to actively participate in pertinent portions of the program?

0901i

10. Does the program include audience testing by means of skits and hypothetical situations?

0901b

11. Does the program include the use of posters, placards, and leaflets in conspicuous locations throughout the activity?

0901f

16 SEP 1985

CHAPTER 9

PART 2

SECURITY FORCE TRAINING

YES NO N/A REF

1. Does the activity provide prescribed security force training including:

a. An eight week security force training curriculum styled on Appendix XIII?

0903

b. Specialized, advanced security force training?

0903b

During the past 12-month period, how many security force personnel received training in:

locksmith training_____

IDS training_____

anti-terrorism training_____

loss prevention training_____

2. Does the activity have a designated security force training coordinator?

0903

3. Are there adequate lesson plans in use to cover all facets of security and law enforcement, as prescribed?

0903

4. Does the activity provide for training of security force personnel at the Federal Law Enforcement Training Center, Glynco, GA?

0904

5. Does the activity provide for training of security force personnel at the U.S. Army Military Police School, Ft. McClellan, AL?

0904

6. Is "outside" law enforcement/security training provided at schools/academies other than 4 and 5 above?

0904

If yes, name of school(s)_____

7. Are security force personnel required to complete the emergency vehicle driver training?

0910

YES NO N/A REF

8. Are local agreements and/or licenses provided security force personnel who operate security vehicles in areas of concurrent or proprietary legislative jurisdiction?

If no, has the activity obtained written exemptions from local or state law enforcement agencies?

09050

9. Are individual training records adequately maintained for security force personnel?

0908

10. Has a field training officer (FTO) been designated?

0907

11. Do supervisors and the FTO periodically evaluate the training program for effectiveness and currency?

09070

a. If yes, how often are evaluations made?

12. Is there a security force Roll Call training program?

09120

13. Are installation maps conspicuously posted and provided security force personnel indicating types and locations of legislative jurisdictions?

14. Are all members of the security force provided a security handbook?

0908

15. Does the activity provide adequate training for the Crisis Response Force (CRF)?

0909

16. Does the CRF training include periodic alerts and rehearsals of the emergency and disaster contingency plans?

0909

17. Do all security force personnel required to bear firearms receive training?

0900

18. Does firearm training include individual firearms proficiency?

0900

a. Are all security force personnel required to qualify initially and annually thereafter?

0913,
091

SEP 1985

YES NO N/A REF

- b. Do all security force personnel receive quarterly firearm familiarization training?
- c. Are firearms and ammunition not in-service stored and controlled in accordance with OPNAVINST 5530.13?
- d. Are in-service firearms and ammunition at security departments stored in accordance with NAVINST 5530.13?
- e. Is each security force member assigned his/her individual firearm?
- f. Is the weapon/weapon custody receipt card change system used?
- g. Are all in-service weapons inventoried, inspected, and receipted for at conclusion/commencement of each shift?
- h. Are quarterly inventories of all weapons assigned the security department conducted by the security officer or designated representative?
- i. Are annual firearm inventories of all weapons assigned the activity conducted by the security officer or as prescribed in NAVMATINST 5530.1A?
- j. Are copies of all firearms inventories maintained by the security officer for at least two years?
- k. Are firearm proficiency achievement awards issued to uniformed security force personnel in accordance with CMMI 594?
- l. Do all security force personnel receive adequate indoctrination in the use of force quarterly and annually in concert with firearms qualification/familiarization?
- m. Do DOD civilian security force personnel comply with prescribed uniform requirements?
- n. Do military security force personnel comply with Naval Uniform Regulations?

0914

0913

CHAPTER 10

SECURITY FORCE COMMUNICATIONS

YES NO N/A REF

1. Does the activity security force have its own communications system with direct communications between security headquarters and security elements? 1000
2. Is there an auxiliary power supply for the communications with each element of the security force? 1000/
1003
3. Is there sufficient equipment to maintain continuous communications with each element of the security force? 1000
4. Is there adequate alternate means of communications available to the security force? 1000
5. What is the primary means of communication for the security force? _____
The alternate means? _____
6. Radio communications:
 - a. Are proper radio procedures practiced?
 - b. Is an effective routine code being used (such as the "10" code)? 1001a
 - c. Is all communications equipment properly maintained? 1003a
 - d. Are there at least two dedicated radio frequencies for security force use? 1003a
 - e. Are handi-talkies equipped with multiple-frequency capability? 1003a
 - f. Are handi-talkies equipped with an automatic-tilt or switch activated duress frequency?
7. Does the security force use a duress code for emergency situations? 1003a

OPNAVINST 5530.14A

16 SEP 1985

YES NO N/A REF

a. Is the duress code changed at least
monthly?

1003a

8. Is the communications center afforded adequate
physical security against armed intrusion?

1003a

9. Are communications systems capable of being
used to transmit instructions to all key posts
simultaneously in a rapid and timely manner?

1003a

CHAPTER 11

SECURITY DEVICES AND EQUIPMENT

YES NO N/A REF

1. Does the security force have sufficient, adequately equipped vehicles to maintain patrols, respond to alarms and emergencies, and maintain supervision? 1101
 - a. Are security force vehicles equipped with:
 - (1) Signs conspicuously identifying the vehicle as a security police vehicle? 1101
 - (2) Red and/or blue emergency exterior overhead lights? 1101
 - (3) Electronic siren? 1101
 - (4) Electronic latch shotgun holder? 1101
 - b. Do security force vehicles have relatively low mileage? 1101
2. How often do the security officer and supervisory personnel review the firearms and ammunition requirements to ensure their adequacy? 1102

3. Does the security officer have a copy of NAVMAT Instruction 8300.1A?
4. Do observation towers provide security personnel with adequate observation of security areas? 1103a
5. Are observation towers equipped with:
 - a. Bullet resistant material to waist height? 1103b
 - b. Portholes and trap doors? 1103b
 - c. An IDS pressure sensor to detect unauthorized use of stairs to towers? 1103b
6. Is only standard propellant load and fully jacketed ball design ammunition used by armed security force personnel? 1102a

YES NO N/A RE

7. Is ammunition properly secured and issued only for authorized purposes?

OPNAVINST
5530.13

8. Are weapons stored in arms racks or containers and adequately secured when not in use?

OPNAVINST
5530.13

9. Are duties other than those related to security performed by security force personnel?

10. Does the activity have a military working dog program?

110

a. Has the program been approved by the Chief of Naval Operations?

110

11. Does the activity provide devices and specialized equipment for use by the security force?

110

12. Does the activity provide security force personnel with individual equipment?

110

APPENDIX IX
PART 1

AVIATION ASSETS

1. This Appendix sets forth minimum physical security requirements for aviation assets ashore. For purposes of this instruction, aviation assets include:
 - a. Aircraft
 - b. Aircraft flightlines
 - c. Ramps
 - d. Control towers
 - e. Rework facilities
 - f. Ancilliary equipment and facilities
2. Aviation asset areas will be designated as Limited Areas and must be protected against Threat Types ONE through FIVE.
3. In addition to the requirements contained in paragraph 0306c(2) and the remainder of the basic instruction, aviation assets will be protected as follows:
 - a. Perimeter. The perimeter/perimeter barrier will be protected by one or more electronic security sensor systems. Such systems will terminate in an alarm control center within the protected area.
 - b. Clear Zones. Clear zones of 30 feet (9 meters) on the interior and 20 feet (6 meters) on the exterior are required. Greater clear zones are encouraged.
 - c. Alarm Verification. The capability must exist for realtime assessment of alarm activations of the perimeter. Closed circuit television (CCTV), guards in observation towers, or a response force may be used to accomplish this.
 - d. Response. At least two on-duty security force members will be present at all times within the Limited Area or located in close proximity. The purpose of this team is to provide initial rapid response to intrusion detection system violations and other emergency situations. The team will be equipped with a security communications system meeting the criteria contained in Chapter 10 and will be mobile or have adequate vehicles immediately available for emergency response situations.

ters. At water perimeters where fencing is
ity will be provided by one or more of the

trol craft manned by security force

urveillance by security force personnel,
rvation towers, or combinations thereof.

ic waterside security systems (when

16 SEP 1985

APPENDIX IXPART 2NAVY SHIPYARDSCONTROLLED INDUSTRIAL AREA (CIA)

1. This appendix sets forth minimum physical security requirements for Navy shipyard Controlled Industrial Areas (CIA). CIAs will be designated as Limited Areas and protected against Threat Types ONE through FIVE.

2. In addition to the requirements contained in paragraph 0306c(2) and the remainder of the basic instruction, shipyard CIAs will be protected as follows:

a. Perimeter. The perimeter/perimeter barrier will be protected by one or more electronic security sensor systems. Such systems will terminate in an alarm control center within the protected area.

b. Clear Zones. Because most shipyards have been at their present locations for many years and have grown increasingly larger while surrounding communities have expanded closer to the shipyards, the clear zone requirements of Chapter 6 cannot be met. Accordingly, shipyards are exempt from such clear zone requirements. Combined clear zones of 20 feet (6 meters) consisting of 10 feet (3 meters) on the interior and 10 feet (3 meters) on the exterior will be maintained. Naval shipyards incapable of meeting these clear zone requirements must implement compensatory measures based upon Chapter 6 guidelines (these clear zone requirements apply to shipyard outer perimeters as well as CIAs).

c. Alarm Verification. The capability must exist for realtime assessment of alarm activations of the perimeter. Closed circuit television (CCTV), guards in observation towers, or a response force may be used to accomplish this.

d. Response. At least two on-duty security force members will be present at all times within the CIA or located in close proximity. The purpose of this team is to provide initial rapid response to intrusion detection system violations and other emergency situations. The team will be equipped with a security communications system meeting the criteria contained in Chapter 10 and will be mobile or have adequate vehicles immediately available for emergency response situations.

e. Water Perimeters. At water perimeters where fencing is not practical, security will be provided by one or more of the following:

OPNAVINST 5530.14A

16 SEP 1985

(1) Water patrol craft manned by security force personnel.

(2) Visual surveillance by security force personnel, CCTV, guards in observation towers, or combinations thereof.

(3) Electronic waterside security systems (when available).

16 SEP 1985

APPENDIX IX
PART 3

COMMUNICATIONS STATIONS

1. This appendix sets forth minimum physical security requirements for communication stations. Communication stations will be designated, as a minimum, Controlled Areas and be protected against Threat Types ONE through FIVE. Facilities housing receivers, transmitters, communication centers, and related functions will be designated and protected as Limited Areas.

2. In addition to the requirements contained in paragraph 0306c(3) and the remainder of the basic instruction, communication assets will be protected as follows:

a. Perimeter. There may be situations whereby fencing a communication station is neither practical nor cost effective. An example would be where several antenna fields are located thereon. In such situations, consideration should be given to condensing (or reducing) the size of the Controlled Area and providing proper protection. An alternative is to establish fixed security guard posts at the perimeter and conducting frequent security patrols.

b. Clear Zones. Minimum clear zones of 30 feet (9 meters) on the interior and 20 feet (6 meters) on the exterior are required. Greater clear zones, particularly on the exterior, are encouraged.

c. Alarm Verification. Where the perimeter is protected with electronic security sensor systems, the capability must exist for realtime assessment of alarm activations. Closed circuit television (CCTV), guards in observation towers or a response force may be used to accomplish this.

d. Response. At least two on-duty security force members will be present at all times within the Controlled Area or located in close proximity. The purpose of this team is to provide initial rapid response to intrusion detection system violations and other emergency situations. The team will be equipped with a security communications system meeting the criteria contained in Chapter 10 and will be mobile or have adequate vehicles immediately available for emergency response situations.

3. In cases where naval communications facilities are tenant activities aboard naval stations or naval air stations previously delineated security requirements may be relaxed to the extent that the requisite security is provided by the host installation.

16 SEP 1985

APPENDIX IX
PART 4

WATERFRONT SECURITY

1. This Appendix sets forth minimum physical security standards for waterfronts, to include piers and wharves servicing ships. Such areas will be designated, as a minimum, Controlled Areas. They must be protected against Threat Types ONE through FIVE.

2. In addition to the requirements contained in paragraph 0306c(3) and the remainder of the basic instruction, waterfronts will be protected as follows:

a. Barriers. Barriers will be provided to prevent direct unchallenged access into piers and wharves when ships are moored.

b. Vehicle Access. Vehicular ingress/egress to piers and wharves will be controlled. Parking of vehicles on piers and wharves will be limited to essential government or commercial vehicles. Where vehicle parking is necessary on piers and wharves, such parking will be separated by a barrier a minimum of 30 feet (9 meters) from in port ships.

c. Threat Planning. Security planning will address measures to implement increasingly stringent access control during increased THREATCON situations.

d. Response. At least two on-duty security force members will be present at all times within the Controlled Area or located in close proximity. The purpose of this team is to provide initial rapid response to intrusion detection system violations and other emergency situations. The team will be equipped with a security communications system meeting the criteria contained in Chapter 10 and will be mobile or have adequate vehicles immediately available for emergency response situations.

e. Water Boundaries. At water boundaries where physical barriers are impractical, security for in port ships will be provided by one or more of the following:

(1) Water patrol craft manned by security force personnel.

(2) Visual surveillance by security force personnel, closed circuit television, guards in observation towers or guards on foot on piers and/or ships, or combinations thereof.

OPNAVINST 5530.14A
16 SEP 1985

(3) Electronic waterside security systems (when available).

APPENDIX IX
PART 5

POL

BULK FUEL STORAGE AREAS

1. This Appendix sets forth guidelines and minimum physical security standards for bulk storage areas. Such areas will be designated as Controlled Areas and must be protected to the degree set forth in paragraph 0306c(3).

2. In addition to the requirements contained in paragraph 0306c(3) and the remainder of the basic instruction, bulk fuel storage areas will be protected as follows:

a. Perimeter/Area. The perimeter and area will be randomly patrolled by security force personnel a minimum of three times per eight hour shift. An electronic intrusion detection system (IDS) may be used to protect the perimeter. If an IDS is used, the system will terminate in an alarm control center located on the installation or at the supporting military activity/installation. Two-way radio voice communications shall exist between the alarm control center and patrol units capable of realtime response to an alarm activation.

b. Clear Zones. Clear zones will be established and maintained as outlined in paragraph 0606. Greater clear zones are encouraged.

c. Response. At least two on-duty security force members will be present at all times within the Controlled Area or located in close proximity. The purpose of this team is to provide initial rapid response to intrusion detection system violations and other emergency situations. The team will be equipped with a security communications system meeting the criteria contained in Chapter 10 and will be mobile or have adequate vehicles immediately available for emergency response situations.

16 SEP 1985

APPENDIX X

21 CODE OF FEDERAL REGULATIONS, PART 1308

The Code of Federal Regulations is subject to frequent change, and this Appendix should be consulted for general guidance only.

§ 1307.31**SPECIAL EXEMPT PERSONS****§ 1307.31 Native American Church.**

The listing of peyote as a controlled substance in Schedule I does not apply to the nondrug use of peyote in bona fide religious ceremonies of the Native American Church, and members of the Native American Church so using peyote are exempt from registration. Any person who manufactures peyote for or distributes peyote to the Native American Church, however, is required to obtain registration annually and to comply with all other requirements of law.

PART 1308—SCHEDULES OF CONTROLLED SUBSTANCES**GENERAL INFORMATION**

- Sec.
1308.01 Scope of Part 1308.
1308.02 Definitions.
1308.03 Administration Controlled Substances Code Number.
1308.04 Submission of information by manufacturers.

SCHEDULES

- 1308.11 Schedule I.
1308.12 Schedule II.
1308.13 Schedule III.
1308.14 Schedule IV.
1308.15 Schedule V.

EXCLUDED NONNARCOTIC SUBSTANCES

- 1308.21 Application for exclusion of a non-narcotic substance.
1308.22 Excluded substances.

EXEMPT CHEMICAL PREPARATIONS

- 1308.23 Exemption of certain chemical preparations; application.
1308.24 Exemption chemical preparations.

EXCEPTED STIMULANT OR DEPRESSANT COMPOUNDS

- 1308.31 Application for exception of a stimulant or depressant compound.
1308.32 Excepted compounds.

HEARINGS

- 1308.41 Hearings generally.
1308.42 Purpose of hearing.
1308.43 Waiver or modification of Rules.
1308.44 Initiation of proceedings for rule-making.
1308.45 Request for hearing or appearance; waiver.

Title 21—Food and Drugs**Sec.**

- 1308.47 Time and place of hearing.
1308.48 Final order.
1308.49 Control required under international treaty.
1308.50 Control of immediate precursors.
1308.51 Pending proceedings.

AUTHORITY: Secs. 201, 202, 501(b), 84 Stat. 1245, 1246, 1247, 1248, 1249, 1250, 1251, 1252, 1271, 21 U.S.C. 811, 812, 871(b).

SOURCE: 38 FR 8254, Mar. 30, 1973. Redesignated at 38 FR 26609, Sept. 24, 1973, unless otherwise noted.

NOMENCLATURE CHANGES: 38 FR 26609, Sept. 24, 1973.

GENERAL INFORMATION**§ 1308.01 Scope of Part 1308.**

Schedules of controlled substances established by section 202 of the Act (21 U.S.C. 812), as they are changed, updated, and republished from time to time, are set forth in this part.

§ 1308.02 Definitions.

As used in this part, the following terms shall have the meanings specified:

(a) The term "Act" means the Controlled Substance Act (84 Stat. 1242; 21 U.S.C. 801) and/or the Controlled Substances Import and Export Act (84 Stat. 1285; 21 U.S.C. 951).

(b) The term "hearing" means any hearing held pursuant to this part for the issuance, amendment, or repeal of any rule issuable pursuant to section 201 of the Act.

(c) The term "isomer" means, except as used in § 1308.11(d), the optical isomer. As issued in § 1308.11(d), the term "isomer" means the optical, position or geometric isomer.

(d) The term "interested person" means any person adversely affected or aggrieved by any rule or proposed rule issuable pursuant to section 201 of the Act.

(e) The term "proceeding" means all actions taken for the issuance, amendment, or repeal of any rule issued pursuant to section 201 of the Act, commencing with the publication by the Administrator of the proposed rule, amended rule, or repeal in the **FEDERAL REGISTER**.

(f) Any term not defined in this section shall have the definition set forth

Chapter II—Drug Enforcement Admin., Dept. of Justice

§ 1308.11

in section 102 and 1001 of the Act (21 U.S.C. 802 and 951) and § 1301.02 of this chapter.

§ 1308.03 Administration Controlled Substances Code Number.

(a) Each controlled substance, or basic class thereof, has been assigned a "Administration Controlled Substances Code Number" for purposes of identification of the substances or class on certain Certificates of Registration issued by the Administration pursuant to § 1301.44 of this chapter and on certain order forms issued by the Administration pursuant to § 1305.05(d) of this chapter. Certain applicants for registration must include the appropriate numbers on the application as required in § 1301.32(d) and applicants for procurement and/or individual manufacturing quotas must include the appropriate number on the application as required in §§ 1303.12(b) and 1303.22(a).

(b) Except as stated in paragraph (a) of this section, no applicant or registrant is required to use the Administration Controlled Substances Code Number for any purpose.

§ 1308.04 Submission of information by manufacturers.

(a) Each person who manufactures, packages, repackages, labels, relabels, or distributes under his own label any product (including any compound, mixture, or preparation, diagnostic, reagent, buffer, or biological) containing any quantity of any controlled substance (whether such product is itself controlled or is excepted, exempted, or excluded from some or all controls pursuant to § 1308.21-24 or § 1308.31-32) shall submit information required in paragraph (b) of this section for each such product being manufactured or sold on July 1, 1972. The information should be submitted by registered mail, return receipt requested, to the Regulatory Support Division, Attention: Project Label, Drug Enforcement Administration, Department of Justice, Washington, D.C. 20537, by August 31, 1972. In the case of new products manufactured after July 1, 1972, or new dosage forms or other unit forms manufactured after July 1, 1972, or changes in information

submitted by August 31, 1972, the registrant shall submit the information regarding such item within 30 days after the date on which the manufacture commences or information change occurs. In the case of products, the manufacture of which is discontinued after July 1, 1972, the registrant shall submit notice of such discontinuance within 30 days after the date on which manufacture ceases. In the case of products the manufacture of which was discontinued before July 1, 1972, which are still being sold, the registrant shall submit a notice of such discontinuance with his initial submission.

(b) Two labels or other documents reflecting the following information shall be submitted with reference to each dosage form or other unit form of each item containing any quantity of any controlled substance:

(1) The trade name, brand name, or other commercial name of the product;

(2) The generic or chemical name and quantity of each active ingredient, including both controlled and noncontrolled substances (if any of this information is a proprietary trade secret, please indicate those portions);

(3) The National Drug Code Number assigned to the product, if any; and

(4) The weight (in metric measure) of each dosage unit or the weight (in metric measure) of the controlled substance per 100 grams of finished product for all items containing any quantity of any narcotic controlled substance in solid dosage forms.

(21 U.S.C. 821 and 871(b))

[38 FR 8254, Mar. 30, 1973. Redesignated at 38 FR 26609, Sept. 24, 1973, and amended at 46 FR 28841, May 29, 1981]

SCHEDULES

§ 1308.11 Schedule I.

(a) Schedule I shall consist of the drugs and other substances, by whatever official name, common or usual name, chemical name, or brand name designated, listed in this section. Each drug or substance has been assigned the DEA Controlled Substances Code Number set forth opposite it.

16 SEP 1985

§ 1308.11

(b) *Opiates*. Unless specifically excepted or unless listed in another schedule, any of the following opiates, including their isomers, esters, ethers, salts, and salts of isomers, esters, and ethers, whenever the existence of such isomers, esters, ethers, salts is possible within the specific chemical designation:

(1) Acetylmeadol.....	9801
(2) Allyprodine.....	9802
(3) Alphaacetylmeadol.....	9803
(4) Alphameprodine.....	9804
(5) Alphameadol.....	9805
(6) Alpha-methylpentanyl (N-[1-(alpha-methyl-beta-phenylethyl-4-piperidyl) propionanilide; 1-(1-methyl-2-phenylethyl)-4-(N-propenilido) piperidine].....	9814
(7) Benzethidine.....	9806
(8) Betaacetylmeadol.....	9807
(9) Betameprodine.....	9808
(10) Betameadol.....	9809
(11) Betaprodine.....	9811
(12) Clonitazene.....	9812
(13) Dextromoramide.....	9813
(14) Diampromide.....	9815
(15) Diethylthiambutene.....	9816
(16) Difenoxin.....	9818
(17) Dimenoxadol.....	9817
(18) Dimpheptanol.....	9818
(19) Dimethylthiambutene.....	9819
(20) Dioxaphetyl butyrate.....	9821
(21) Dipipanone.....	9822
(22) Ethylmethylthiambutene.....	9823
(23) Etomidate.....	9824
(24) Etomidine.....	9825
(25) Furethidine.....	9826
(26) Hydroxypethidine.....	9827
(27) Ketobemidone.....	9828
(28) Levomoramide.....	9829
(29) Levophencylmorphan.....	9831
(30) Morpheridine.....	9832
(31) Noracymethadol.....	9833
(32) Norlevorphanol.....	9834
(33) Normethadone.....	9835
(34) Norpipanone.....	9836
(35) Phenadoxone.....	9837
(36) Phenampromide.....	9838
(37) Phenomorphan.....	9847
(38) Phenoperidine.....	9841
(39) Pirtramide.....	9842
(40) Proheptazine.....	9843
(41) Propetidine.....	9844
(42) Propiram.....	9849
(43) Racemoramide.....	9845
(44) Sufentanil.....	9740
(45) Tilidine.....	9750
(46) Trimeperidine.....	9846

(c) *Opium derivatives*. Unless specifically excepted or unless listed in another schedule, any of the following opium derivatives, its salts, isomers, and salts of isomers whenever the existence of such salts, isomers, and salts of isomers is possible within the specific chemical designation:

Title 21—Food and Drugs

(1) Acetorphine.....	9318
(2) Acetyldihydrocodeine.....	9361
(3) Benzylmorphine.....	9352
(4) Codeine methylbromide.....	9370
(5) Codeine-N-Oxide.....	9363
(6) Cyrenorphine.....	9364
(7) Desomorphine.....	9355
(8) Dihydromorphine.....	9145
(9) Drosteanol.....	9335
(10) Etorphine (except hydrochloride salt).....	9366
(11) Heroin.....	9200
(12) Hydromorphanol.....	9301
(13) Methyldeorphine.....	9302
(14) Methylhydromorphine.....	9304
(15) Morphine methylbromide.....	9305
(16) Morphine methylsulfonate.....	9306
(17) Morphine-N-Oxide.....	9307
(18) Myrophine.....	9308
(19) Nicocodine.....	9309
(20) Nicomorphine.....	9312
(21) Normorphine.....	9313
(22) Pholcodine.....	9314
(23) Thebacon.....	9315

(d) *Hallucinogenic substances*.

Unless specifically excepted or unless listed in another schedule, any material, compound, mixture, or preparation, which contains any quantity of the following hallucinogenic substances, or which contains any of its salts, isomers, and salts of isomers whenever the existence of such salts, isomers, and salts of isomers is possible within the specific chemical designation (for purposes of this paragraph only, the term "isomer" includes the optical, position and geometric isomers):

(1) 4-bromo-2,5-dimethoxy-amphetamine.....	7391
Some trade or other names: 4-bromo-2,5-dimethoxy- α -methylphenethylamine; 4-bromo-2,5-DMA	
(2) 2,5-dimethoxyamphetamine.....	7396
Some trade or other names: 2,5-dimethoxy- α -methylphenethylamine; 2,5-DMA	
(3) 4-methoxyamphetamine.....	7411
Some trade or other names: 4-methoxy- α -methylphenethylamine; paramethoxyamphetamine, PMA	
(4) 5-methoxy-3,4-methylenedioxy-amphetamine.....	7401
(5) 4-methyl-2,5-dimethoxy-amphetamine.....	7395
Some trade and other names: 4-methyl-2,5-dimethoxy- α -methylphenethylamine; "DOM"; and "STP"	
(6) 3,4-methylenedioxy amphetamine.....	7400
(7) 3,4,5-trimethoxy amphetamine.....	7390
(8) Bufotenine.....	7423
Some trade and other names: 3-(β -Dimethylaminoethoxy)-5-hydroxyindole, 3-(2-dimethylaminoethoxy)-5-indolol; N, N-dimethylserotonin, 5-hydroxy-N,N-dimethyltryptamine; mappine	
(9) Diethyltryptamine.....	7434
Some trade and other names: N,N-Diethyltryptamine; DET	
(10) Dimethyltryptamine.....	7435
Some trade or other names: DMT	
(11) Ibogaine.....	7280
Some trade and other names: 7-Ethyl-6,6,7,8,9,10,12,13-octahydro-2-methoxy-6,9-methano-5H-pyrido [1', 2':1,2] esapino [5,4-b] indole; Tabernanthe iboga	
(12) Lysergic acid diethylamide.....	7315

16 SEP 1985

Chapter II—Drug Enforcement Admin., Dept. of Justice

§ 1308.12

(13) Marijuana.....	7360
(14) Mescaline.....	7361
(15) Parahexyl—7374; some trade or other names: 3-Hexyl-1-hydroxy-7,8,9,10-tetrahydro-6,6,9-trimethyl-6H-benzo[b,d]pyran; Synhexyl.....	7415
(16) Peyote.....	7437
Meaning all parts of the plant presently classified botanically as <i>Lophophora williamsii</i> Lemaire, whether growing or not, the seeds thereof, any extract from any part of such plant, and every compound, manufacture, salts, derivative, mixture, or preparation of such plant, its seeds or extracts	
Interprets 21 USC 812(c), Schedule I(c) (12))	
(17) N-ethyl-3-piperidyl benzilate.....	7482
(18) N-methyl-3-piperidyl benzilate.....	7484
(19) Palococyl.....	7437
(20) Palococyl.....	7438
(21) Tetrahydrocannabinols.....	7370
Synthetic equivalents of the substances contained in the plant, or in the resinous extractives of <i>Cannabis</i> , sp. and/or synthetic substances, derivatives, and their isomers with similar chemical structure and pharmacological activity such as the following:	
Δ1 cis or trans tetrahydrocannabinol, and their optical isomers	
Δ6 cis or trans tetrahydrocannabinol, and their optical isomers	
Δ3,4 cis or trans tetrahydrocannabinol, and its optical isomers	
(Since nomenclature of these substances is not internationally standardized, compounds of these structures, regardless of numerical designation of steric positions covered.)	
(22) Ethylamine analog of phencyclidine.....	7455
Some trade or other names: N-ethyl-1-phenylcyclohexylamine, (1-phenylcyclohexyl)ethylamine, N-(1-phenylcyclohexyl)ethylamine, cyclohexamine, PCE	
(23) Pyrrolidine analog of phencyclidine.....	7458
Some trade or other names: 1-(1-phenylcyclohexyl)-pyrrolidine, PCPy, PHP	
(24) Thiophene analog of phencyclidine.....	7470
Some trade or other names: 1-[1-(2-thienyl)-cyclohexyl]-piperidine, 2-thienylanalog of phencyclidine, TPCP, TCP	

(e) **Depressants.** Unless specifically excepted or unless listed in another schedule, any material, compound, mixture, or preparation which contains any quantity of the following substances having a depressant effect on the central nervous system, including its salts, isomers, and salts of isomers whenever the existence of such salts, isomers, and salts of isomers is possible within the specific chemical designation:

(1) Mecloqualone.....	2572
-----------------------	------

(f) **Stimulants.** Unless specifically excepted or unless listed in another schedule, any material, compound, mixture, or preparation which contains any quantity of the following substances having a stimulant effect

on the central nervous system, including its salts, isomers, and salts of isomers:

(1) Fenethylamine.....	1503
(2) N-ethylamphetamine.....	1475

[39 FR 22141, June 20, 1974]

EDITORIAL NOTE: For Federal Register citations affecting § 1308.11, see the List of CFR Sections Affected in the Finding Aids section of this volume.

§ 1308.12 Schedule II.

(a) Schedule II shall consist of the drugs and other substances, by whatever official name, common or usual name, chemical name, or brand name designated, listed in this section. Each drug or substance has been assigned the Controlled Substances Code Number set forth opposite it.

(b) Substances, vegetable origin or chemical synthesis. Unless specifically excepted or unless listed in another schedule, any of the following substances whether produced directly or indirectly by extraction from substances of vegetable origin, or independently by means of chemical synthesis, or by a combination of extraction and chemical synthesis:

(1) Opium and opiate, and any salt, compound, derivative, or preparation of opium or opiate, excluding apomorphine, dextrorphan, nalbuphine, naloxone, and naltrexone, and their respective salts, but including the following:

1 Raw opium.....	9600
2 Opium extracts.....	9610
3 Opium fluid extracts.....	9620
4 Powdered opium.....	9639
5 Granulated opium.....	9640
6 Tincture of opium.....	9630
7 Codeine.....	9050
8 Ethylmorphine.....	9190
9 Etorphine hydrochloride.....	9059
10 Hydrocodone.....	9193
11 Hydromorphone.....	9150
12 Metopon.....	9260
13 Morphine.....	9300
14 Oxycodone.....	9143
15 Oxymorphone.....	9652
16 Thebaine.....	9333

(2) Any salt, compound, derivative, or preparation thereof which is chemically equivalent or identical with any of the substances referred to in para-

16 SEP 1985

§ 1308.13

graph (b) (1) of this section, except that these substances shall not include the isoquinoline alkaloids of opium.

(3) Opium poppy and poppy straw.

(4) Coca leaves (9040) and any salt, compound, derivative, or preparation of coca leaves, and any salt, compound, derivative, or preparation thereof which is chemically equivalent or identical with any of these substances, except that the substances shall not include decocainized coca leaves or extraction of coca leaves, which extractions do not contain cocaine (9041) or ecgonine (9180).

(5) Concentrate of poppy straw (the crude extract of poppy straw in either liquid, solid or powder form which contains the phenanthrene alkaloids of the opium poppy), 9670.

(c) *Opiates*. Unless specifically excepted or unless in another schedule any of the following opiates, including its isomers, esters, ethers, salts and salts of isomers, esters and ethers whenever the existence of such isomers, esters, ethers, and salts is possible within the specific chemical designation, dextrorphan and levopropoxyphene excepted:

(1) Alphaprodine.....	9010
(2) Anileridine.....	9020
(3) Bextramide.....	9000
(4) Bulk dextropropoxyphene (non-dosage forms).....	9273
(5) Dihydrocodaine.....	9120
(6) Diphenoxylate.....	9170
(7) Fentanyl.....	9801
(8) Isomethadone.....	9226
(9) Levomethorphan.....	9210
(10) Levorphanol.....	9220
(11) Mebazocine.....	9240
(12) Methadone.....	9250
(13) Methadone-intermediate, 4-cyano-2-dimethyl- mino-4,4-diphenyl butane.....	9254
(14) Moramide-intermediate, 2-methyl-3-morpholino-1, 1-diphenylpropane-carboxylic acid.....	9802
(15) Pethidine (meperidine).....	9230
(16) Pethidine-intermediate-A, 4-cyano-1-methyl-4- phenylpiperidine.....	9232
(17) Pethidine-intermediate-B, ethyl-4-phenylpiperi- dine-4-carboxylate.....	9233
(18) Pethidine-intermediate-C, 1-methyl-4-phenylpiperi- dine-4-carboxylic acid.....	9234
(19) Phenazocine.....	9715
(20) Piminodine.....	9730
(21) Racemethorphan.....	9732
(22) Racemorphane.....	9733

(d) *Stimulants*. Unless specifically excepted or unless listed in another schedule, any material, compound, mixture, or preparation which contains any quantity of the following

Title 21—Food and Drugs

substances having a stimulant effect on the central nervous system:

(1) Amphetamine, its salts, optical isomers, and salts of its optical isomers.....	1100
(2) Methamphetamine, its salts, isomers, and salts of its isomers.....	1105
(3) Phenmetrazine and its salts.....	1631
(4) Methyphenidate.....	1724

(e) *Depressants*. Unless specifically excepted or unless listed in another schedule, any material, compound, mixture, or preparation which contains any quantity of the following substances having a depressant effect on the central nervous system, including its salts, isomers, and salts of isomers whenever the existence of such salts, isomers, and salts of isomers is possible within the specific chemical designation:

(1) Amobarbital.....	2125
(2) Methaqualone.....	2366
(3) Penobarbital.....	2270
(4) Phencyclidine.....	7471
(5) Secobarbital.....	2315

(f) *Immediate precursors*. Unless specifically excepted or unless listed in another schedule, any material, compound, mixture, or preparation which contains any quantity of the following substances:

(1) Immediate precursor to amphetamine and methamphetamine:

(i) Phenylisotone.....	9801
Some trade or other names: phenyl-2-propanone; P2P; benzyl methyl ketone; methyl benzyl ketone;	

(2) Immediate precursors to phencyclidine (PCP):

(i) 1-phenylcyclohexylamine.....	7480
(ii) 1-piperidinocyclohexanecarbonitrile (PCC).....	9803

[39 FR 22142, June 20, 1974]

NOTE: For Federal Register citations affecting § 1308.12, see the List of CFR Sections Affected in the Finding Aids section of this volume.

§ 1308.13 Schedule III.

(a) Schedule III shall consist of the drugs and other substances, by what-

Chapter II—Drug Enforcement Admin., Dept. of Justice

§ 1308.14

ever official name, common or usual name, chemical name, or brand name designated, listed in this section. Each drug or substance has been assigned the DEA Controlled Substances Code Number set forth opposite it.

(b) *Stimulants*. Unless specifically excepted or unless listed in another schedule, any material, compound, mixture, or preparation which contains any quantity of the following substances having a stimulant effect on the central nervous system, including its salts, isomers (whether optical, position, or geometric), and salts of such isomers whenever the existence of such salts, isomers, and salts of isomers is possible within the specific chemical designation:

(1) Those compounds, mixtures, or preparations in dosage unit form containing any stimulant substances listed in schedule II which compounds, mixtures, or preparations were listed on August 25, 1971, as excepted compounds under § 308.32, and any other drug of the quantitative composition shown in that list for those drugs or which is the same except that it contains a lesser quantity of controlled substances.....	1405
(2) Benzphetamine.....	1226
(3) Chlorphentermine.....	1845
(4) Clonidine.....	1647
(5) Phendimetrazine.....	1615

(c) *Depressants*. Unless specifically excepted or unless listed in another schedule, any material, compound, mixture, or preparation which contains any quantity of the following substances having a depressant effect on the central nervous system:

(1) Any compound, mixture or preparation containing:	
(i) Amobarbital.....	2125
(ii) Secobarbital.....	2315
(iii) Pentobarbital.....	2270
or any salt thereof and one or more other active medicinal ingredients which are not listed in any schedule.	
(2) Any suppository dosage form containing:	
(i) Amobarbital.....	2125
(ii) Secobarbital.....	2315
(iii) Pentobarbital.....	2270
or any salt of any of these drugs and approved by the Food and Drug Administration for marketing only as a suppository.	
(3) Any substance which contains any quantity of a derivative of barbituric acid or any salt thereof.....	2100
(4) Chlorhexadol.....	2510
(5) Glutethimide.....	2550
(6) Lysergic acid.....	7300
(7) Lysergic acid amide.....	7310
(8) Methyprylon.....	2575
(9) Sulfonethymethane.....	2600
(10) Sulfonethymethane.....	2605
(11) Sulfonmethane.....	2610

(d) Nalorphine 9400.

(e) *Narcotic Drugs*. Unless specifically excepted or unless listed in another schedule, any material, compound, mixture, or preparation containing any of the following narcotic drugs, or their salts calculated as the free anhydrous base or alkaloid, in limited quantities as set forth below:

(1) Not more than 1.8 grams of codeine per 100 milliliters or not more than 90 milligrams per dosage unit, with an equal or greater quantity of an isoquinoline alkaloid of opium.....	9803
(2) Not more than 1.8 grams of codeine per 100 milliliters or not more than 90 milligrams per dosage unit, with one or more active, nonnarcotic ingredients in recognized therapeutic amounts.....	9804
(3) Not more than 300 milligrams of dihydrocodeinone per 100 milliliters or not more than 15 milligrams per dosage unit, with a fourfold or greater quantity of an isoquinoline alkaloid of opium.....	9805
(4) Not more than 300 milligrams of dihydrocodeinone per 100 milliliters or not more than 15 milligrams per dosage unit, with one or more active, nonnarcotic ingredients in recognized therapeutic amounts.....	9806
(5) Not more than 1.8 grams of dihydrocodeine per 100 milliliters or not more than 90 milligrams per dosage unit, with one or more active, nonnarcotic ingredients in recognized therapeutic amounts.....	9807
(6) Not more than 300 milligrams of ethymorphine per 100 milliliters or not more than 15 milligrams per dosage unit, with one or more active, nonnarcotic ingredients in recognized therapeutic amounts.....	9808
(7) Not more than 500 milligrams of opium per 100 milliliters or per 100 grams or not more than 25 milligrams per dosage unit, with one or more active, nonnarcotic ingredients in recognized therapeutic amounts.....	9809
(8) Not more than 50 milligrams of morphine per 100 milliliters or per 100 grams, with one or more active, nonnarcotic ingredients in recognized therapeutic amounts.....	9810

[39 FR 22142, June 20, 1974, as amended at 41 FR 43401, Oct. 1, 1976; 43 FR 3359, Jan. 25, 1978; 44 FR 40888, July 13, 1979; 46 FR 52334, Oct. 27, 1981]

§ 1308.14 Schedule IV.

(a) Schedule IV shall consist of the drugs and other substances, by whatever official name, common or usual name, chemical name, or brand name designated, listed in this section. Each drug or substance has been assigned the DEA Controlled Substances Code Number set forth opposite it.

(b) *Narcotic drugs*. Unless specifically excepted or unless listed in another schedule, any material, compound, mixture, or preparation containing any of the following narcotic drugs, or their salts calculated as the free anhydrous base or alkaloid, in limited quan-

§ 1308.15

titles as set forth below:

- (1) Not more than 1 milligram of difenoxin (DEA Drug Code No. 9168) and not less than 25 micrograms of atropine sulfate per dosage unit.
- (2) Dextropropoxyphene (alpha-(+)-4-dimethylamino-1,2-diphenyl-3-methyl-2-propionoxybutane)..... 9273

(c) *Depressants.* Unless specifically excepted or unless listed in another schedule, any material, compound, mixture, or preparation which contains any quantity of the following substances, including its salts, isomers, and salts of isomers whenever the existence of such salts, isomers, and salts of isomers is possible within the specific chemical designation:

(1) Alprazolam	2882
(2) Barbitol	2145
(3) Chloral betaine	2480
(4) Chloral hydrate	2485
(5) Chloridazepoxide	2744
(6) Clonazepam	2737
(7) Clorazepate	2768
(8) Diazepam	2765
(9) Ethchlorvynol	2540
(10) Ethinamate	2545
(11) Flurazepam	2787
(12) Halazepam	2782
(13) Lorazepam	2885
(14) Mebutamate	2800
(15) Meprobamate	2820
(16) Methohexital	2264
(17) Methylphenobarbital (mephobarbital)	2250
(18) Oxazepam	2835
(19) Paraldehyde	2585
(20) Petrichloral	2591
(21) Phenobarbital	2285
(22) Prizepam	2764
(23) Temazepam	2825
(24) Triazolam	2887

(d) *Fenfluramine.* Any material, compound, mixture, or preparation which contains any quantity of the following substances, including its salts, isomers (whether optical, position, or geometric), and salts of such isomers, whenever the existence of such salts, isomers, and salts of isomers is possible:

- (1) Fenfluramine

(e) *Stimulants.* Unless specifically excepted or unless listed in another schedule, any material, compound, mixture, or preparation which contains any quantity of the following substances having a stimulant effect on the central nervous system, includ-

Title 21—Food and Drugs

ing its salts, isomers and salts of isomers:

- (1) Diethylpropion..... 1810
- (2) Mazindol..... 1805
- (3) Pemoline (including organometallic complexes and chelates thereof)..... 1830
- (4) Phenamine..... 1840
- (5) Pipradrol..... 1750
- (6) SPA ((-)-1-dimethylamino-1,2-diphenylethane)..... 1835

(f) *Other substances.* Unless specifically excepted or unless listed in another schedule, any material, compound, mixture or preparation which contains any quantity of the following substances, including its salts:

- (1) Pentazocine..... 9709

[39 FR 22143, June 20, 1974]

EDITORIAL NOTE: For Federal Register citations affecting § 1308.14, see the List of CFR Sections Affected in the Finding Aids section of this volume.

§ 1308.15 Schedule V.

(a) Schedule V shall consist of the drugs and other substances, by whatever official name, common or usual name, chemical name, or brand name designated, listed in this section.

(b) Narcotic drugs containing non-narcotic active medicinal ingredients. Any compound, mixture, or preparation containing any of the following narcotic drugs, or their salts calculated as the free anhydrous base or alkaloid, in limited quantities as set forth below, which shall include one or more non-narcotic active medicinal ingredients in sufficient proportion to confer upon the compound, mixture, or preparation valuable medicinal qualities other than those possessed by narcotic drugs alone:

- (1) Not more than 200 milligrams of codeine per 100 milliliters or per 100 grams.
- (2) Not more than 100 milligrams of dihydrocodeine per 100 milliliters or per 100 grams.
- (3) Not more than 100 milligrams of ethylmorphine per 100 milliliters or per 100 grams.
- (4) Not more than 2.5 milligrams of diphenoxylate and not less than 25 mi-

Chapter II—Drug Enforcement Admin., Dept. of Justice

§ 1308.22

crograms of atropine sulfate per dosage unit.

(5) Not more than 100 milligrams of opium per 100 milliliters or per 100 grams.

(6) Not more than 0.5 milligram of difenoxin (DEA Drug Code No. 9168) and not less than 25 micrograms of atropine sulfate per dosage unit. 8010

[39 FR 22143, June 20, 1974, as amended at 43 FR 38383, Aug. 28, 1978; 44 FR 40888, July 13, 1979; 47 FR 49841, Nov. 3, 1982]

EXCLUDED NONNARCOTIC SUBSTANCES

§ 1308.21 Application for exclusion of a nonnarcotic substance.

(a) Any person seeking to have any nonnarcotic substance which may, under the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 301), be lawfully sold over the counter without a prescription, excluded from any schedule, pursuant to section 201(g) (1) of the Act (21 U.S.C. 811 (g) (1)), may apply to the Administrator, Drug Enforcement Administration, Department of Justice, Washington, D.C. 20537.

(b) An application for an exclusion under this section shall contain the following information:

(1) The name and address of the applicant;

(2) The name of the substance for which exclusion is sought; and

(3) The complete quantitative composition of the substance.

(c) Within a reasonable period of time after the receipt of an application for an exclusion under this section, the Administrator shall notify the applicant of his acceptance or non-acceptance of his application, and if not accepted, the reason therefore. The Administrator need not accept an application for filing if any of the requirements prescribed in paragraph (b) of this section is lacking or is not

set forth as to be readily understood. If the applicant desires, he may amend the application to meet the requirements of paragraph (b) of this section. If the application is accepted for filing, the Administrator shall issue and publish in the FEDERAL REGISTER his order on the application, which shall include a reference to the legal authority under which the order is issued and the findings of fact and conclusions of law upon which the order is based. This order shall specify the date on which it shall take effect. The Administrator shall permit any interested person to file written comments on or objections to the order within 60 days of the date of publication of his order in the FEDERAL REGISTER. If any such comments or objections raise significant issues regarding any finding of fact or conclusion of law upon which the order is based, the Administrator shall immediately suspend the effectiveness of the order until he may reconsider the application in light of the comments and objections filed. Thereafter, the Administrator shall reinstate, revoke, or amend his original order as he determines appropriate.

(d) The Administrator may at any time revoke any exclusion granted pursuant to section 201(g) of the Act (21 U.S.C. 811(g)) by following the procedures set forth in paragraph (c) of this section for handling an application for an exclusion which has been accepted for filing.

§ 1308.22 Excluded substances.

The following nonnarcotic substances which may, under the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 301), be lawfully sold over the counter without a prescription, are excluded from all schedules pursuant to section 201(g) (1) of the Act (21 U.S.C. 811(g) (1)):

EXCLUDED NONNARCOTIC OVER-THE-COUNTER SUBSTANCES

Trade name or designation	Dosage form	Composition	Potency	Manufacturer or distributor
Amodrine	Tablet	Phenobarbital	8.00 mg	Searle, G. D. & Co.
		Aminophylline	100.00 mg	
		Racephedrine	25.00 mg	

APPENDIX XI
PARAGRAPH 042351, CHAPTER 2, VOLUME 4
NAVCOMPT MANUAL
(DISBURSING OFFICE SECURITY)
(With minor changes and deletions.)

PROCUREMENT, CUSTODY, AND DISPOSITION OF FUNDS

042351

042351 DISBURSING OFFICE SECURITY

1. GENERAL. The number of accountable positions which require the storing of public funds will be kept to a minimum. Although the guidelines contained herein prescribe the maximum amount of public funds which may be stored in a given container, the actual amount that is stored will depend upon the requirements of the position as calculated in accordance with par. 042301. The maximum amount of security that is available to the disbursing officer will first be used for safeguarding currency, safekeeping of valuables, storing of blank checks, signature plates, undelivered checks, public vouchers, and other records in that order. It is not necessarily advantageous to provide more stringent security measures at times when larger amounts of currency are being stored. Once a security program has been developed for a given area, deviations should be avoided. However, the commanding officer and disbursing officer must continually review the program for obsolescence.

2. RESPONSIBILITY. It is the responsibility of the commanding officer to develop a security program that provides adequate protection for public funds, disbursing documents, disbursing records, and other related disbursing materials. The program should be consistent with the general security of the area in which the disbursing facilities are located and the maximum amount of public funds that will be on hand at any given time. The disbursing officer will ensure that the available disbursing facilities are utilized efficiently so as to provide the greatest amount of protection for the most valuable materials, especially public funds. The security program must include periodic evaluations of the adequacy of security measures being utilized. All security equipment must be tested at least every 6 months for proper operation, and the accountable individual will maintain a record of the tests. It is the responsibility of the disbursing officer to immediately notify the commanding officer of deficiencies in the security program and especially of defective equipment.

3. EXTERNAL SECURITY MEASURES

a. Entry Ways. The number of entry ways via doors and potential entry ways via windows, crawl spaces, etc., will be kept to a minimum and constructed so as to afford reasonable

assurance against forced entry. Sheet metal, security screen, and bars should be utilized where necessary. All screens, hinges, hasps, etc., should be installed with smooth headed bolts and nuts, preferably accessible only from the inside. All exposed bolts, nuts, and hinge pins should be peened in place and jimmy proof or welded.

b. Illumination. Vulnerable exterior areas such as windows, doors, crawl spaces, etc., not visible to normal vehicular or foot traffic should be illuminated at night.

c. Security Patrols. Security patrols will be requested to visually inspect all disbursing containers where possible. At the very least, the area in which the containers are maintained should be inspected regularly.

d. Sentries. The posting of armed guards shall be at the discretion of the commanding officer. However, it is more desirable to utilize other measures, such as alarms, vaults, etc., and in no case should unarmed guards be utilized. Duress alarms or telephonic check-in procedures should be utilized to provide maximum protection for the guards.

e. Keys. Strict accountability of keys allowing access to the disbursing area will be maintained. A record will be maintained which identifies by name all individuals who have been issued keys, along with the dates of issuance and dates on which they are surrendered. Keys which are held for temporary issuance will be maintained by the commanding officer or disbursing officer along with appropriate records regarding their issuance.

4. INTERNAL SECURITY MEASURES

a. Custody. All official currency in the hands of an accountable individual will be kept in a safe or security container as specified in subpar 6. The combination will not be divulged or entrusted in any manner to any other person. When physically incapacitated and unable to open his safe or security container, the accountable individual, upon order of the commanding officer, may divulge the combination to a designated board of officers. Placing the combination in a sealed envelope to be kept in the custody of the commanding officer or any other person is prohibited. Combinations will be changed at least once every 6 months, and a record will be kept that the change has been made. Upon relieving an accountable individual, the replacement will immediately change the combinations of all safes and security containers which he will be using. The dial of the container will be concealed by a shield made of cardboard

or other suitable material so that the operation of the combination cannot be observed by others. The name and phone number of the individual responsible for the contents of the container will be affixed to the inside of the container, or alternatively a unique number of the container and the phone number of a 24-hour duty station will be affixed to the outside of the safe. If the latter option is chosen, the duty station must have access to the individual responsible for the contents.

b. Location. Wherever possible, the storage containers of all persons having custody of funds will be placed in a single room where physical security measures can be concentrated efficiently. A single fund container storage room may be used to compensate for inadequate point security. Whenever possible, public funds or public funds containers will be stored inside a vault. The vault will never be used for open shelved storage of currency. An exception to this requirement is appropriate if the vault is accessible to only one individual. If possible, all containers will be situated so that operation of the combination is not visible to anyone other than the accountable individual. If, of necessity, the container must be placed so that the dial faces an inhabited area, the custodian of the container must shield the dial with his hand or body while operating the combination.

c. Contents. Public funds, disbursing documents or disbursing records will not be stored in a container in which classified material is stored in accordance with reference (a) Paper money will be kept flat and unfolded, according to denominations. It will be arranged uniformly in packages that are marked to indicate the total amount contained in each.

d. Weight. All fund containers which are mounted on wheels or casters or which weigh less than 750 pounds will be secured in such a way as to prevent movement. An exception to the requirement may be appropriate if fund containers are located inside a vault or are protected by an intrusion detection alarm system.

e. Illumination. If the container is visible to the exterior where security patrols pass, illumination will be provided.

f. Work Area. Transactions should be conducted from a cage, room, or counter enclosure, constructed in a manner which will provide a physical barrier to normal traffic and a minimum of interference by other activities and personnel of the office. If the safe or security container is not immediately

accessible, a cash drawer with key lock or other temporary cash storage container should be provided. Whenever the individual using the temporary container leaves the immediate vicinity, the container must be returned to the permanent safe or security container. Access to working areas should be conspicuously marked, where appropriate, for "Authorized Personnel Only". Unauthorized personnel should be prevented from entering the working areas.

5. ALARMS. When security is considered to be inadequate and cannot be upgraded efficiently through other means, intrusion detection alarm systems should be installed and connected to a twenty-four hour command or security post. Alarms should be considered for use to deter entry to the general disbursing area or to the actual storage container. The use of self-contained triggering mechanisms and devices activated in booby-trap fashion is prohibited. The existence of alarms should be well publicized to gain the full benefit of psychological deterrence, and should be identified by conspicuously posted warnings. The installation of an alarm system should be considered when evaluating the physical security of disbursing facilities, especially those with consistently large on-hand cash requirements. Alarms are installed for the purpose of detecting attempts at forced or surreptitious entry and/or to provide a duress system during and after working hours. Alarm systems in and of themselves serve no purpose unless a dedicated response by security or military personnel is accomplished in an expeditious manner. An effective and efficient alarm system should incorporate the following characteristics:

a. capable of promptly detecting forced or surreptitious entry and attempts to tamper with the normal operation of the alarm,

b. flexible for protecting large or small areas with small cost differential,

c. high degree of salvageability for use elsewhere,

d. operate from existing power source and have self-contained, automatic switching capability to an emergency power source in case of power failure,

e. tied to a twenty-four hour security post which can respond within 5 minutes.

f. reasonably immune to nuisance and false alarms or other influences not related to illegal attempts against the protected area or container.

16 SEP 1985

6. STORAGE CONTAINER LIMITATIONS

a. Currency and Negotiable Instruments. Safes or security containers as specified in subpar 7 will be utilized for the following categories of currency and negotiable instruments.

(1) under \$2,000 - The commanding officer will establish fund container requirements. Any of the security containers or burglary resistant safes enumerated in subpar 7 should be used.

(2) \$2,000-\$10,000 - Any of the security containers or safes enumerated in subpar 7 will be used.

(3) \$10,000 - \$50,000 - A security container, as specified in subpar 7a, carrying a Class 1 or Class 5 rating, or a burglary resistant safe as specified in subpar 7b, carrying at least an Underwriters' Laboratories' classification of Tool-Resistant Safe, TL-15 will be used.

(4) \$50,000 or more - A burglary resistant safe, as specified in subparagraph 7b, carrying at least an Underwriters' Laboratories' classification of Tool-Resistant Safe, TL-30 will be used.

b. Other Than Currency and Negotiable Instruments. Safekeeping valuables, blank checks, signature plates, undelivered checks, paid vouchers representing cash, cash books, and other disbursing records and documents must be stored in a security container, as specified in subpar 7a, carrying at least a Class 1 or Class 5 rating or a burglary resistant safe as specified in subpar 7b.

7. CATEGORIES OF STORAGE CONTAINERS

a. Security Containers. General Services Administration approved security containers are manufactured under the following Federal Specifications:

(1) Class 1 or Class 2 cabinet - AA-F-357 (GSA-FSS)

(2) Class 4 or Class 5 cabinet - AA-F-363 (GSA-FSS)

(3) Class 3 or Class 6 Map and Plan File - AA-F-358 (GSA-FSS)

Although all of the foregoing security containers provide protection for any type of contents, they are designed primarily to provide protection for classified material, and as such, are designed to deter entry by individuals utilizing other than

force-entry methods. Of these containers, the Class 1 and Class 5 have been rated to provide protection against forced entry up to 10 man minutes.

b. Burglary Resistant Safes. Commercial burglary resistant safes are certified by Underwriters' Laboratories, according to the following classifications:

- (1) Tool-Resistant Safe - TL-15
- (2) Tool-Resistant Safe - TL-30
- (3) Torch and Tool-Resistant Safe - TRTL-30
- (4) Torch and Tool-Resistant Safe - TRTL-60

The foregoing containers are designed primarily to protect their contents against forced entry. The numerical values utilized in the classifications represent the time, in man minutes, which the given safe should resist forced entry. All of these safes are considered to provide a greater degree of protection than any of the General Services Administration rated security containers.

ALARM SYSTEMS

Section 1.—GENERAL

0501. FOREWORD

Section 2 of this chapter, parts 1 through 6, provides guidelines for the selection of Joint-Service Interior Intrusion Detection System (J-SIIDS) components. Although it is not possible to obtain J-SIIDS components at this time, it is considered appropriate to provide available information with respect to design philosophy, intended usage, and component capabilities. Section 3, parts 1 through 3, provides a listing of some available alarm equipment which may be used pending availability of the J-SIIDS components.

Section 2.—INTRODUCTION

0502. FOREWORD

The J-SIIDS is intended to give in-depth security to the protected room or building. The system is designed with three levels of detection capability in mind. The first level is boundary penetration detec-

tion, the second is motion detection, and the third is point detection. The outermost level, penetration detection, is provided by the penetration sensors and gives the reaction force monitoring the system the earliest notice of an attempted intrusion. The motion sensor provides the second level of protection and detects an intruder only after he has entered the secure area. Thus the allowable response time given the reaction force is shorter than that given by the penetration sensors. The innermost level of detection capability, point detection, is provided by the point sensors. These sensors detect attempted removal of protected items and give the reaction force an allowable response time which is shorter than that given by the first two levels of detection capability. It is recommended that a secure area be provided a minimum of two levels of detection capability. It is further recommended that a particular level, once chosen, be carried to completion; e.g., a room fitted with penetration sensors should be secured against penetration at all points of the room's boundary. Total protection is the predominant factor in system planning.

Part 1. Design Philosophy

0503. GENERAL

The basic J-SIIDS is designed to meet the threat posed by the semiskilled intruder who can be expected to attempt entry without detailed planning or sophisticated equipment and may work individually or as a member of a small group. This intruder can be expected to attack the locks, doors, windows, vents, walls, floors, and ceiling of the protected area, or he may be a "stay-behind" to remove items after the area is secured. He may be expected to resort to robbery by confronting working personnel or guards.

0504. SCOPE

1. *General.* It should be emphasized that an interior intrusion detection system is designed to detect, not

prevent, an attempted intrusion. Thus, a comprehensive physical security plan must contain appropriate physical security measures along with procedures for an effective reaction force. The degree of protection required for a secured area depends on the following:

- a. Threat.
- b. Classification of information being protected.
- c. Location of the room or building.
- d. The construction of the room or building.
- e. The degree of physical security afforded by safes, cabinets, locks, and other supportive security measures.
- f. The effectiveness of the intrusion detection system.

16 SEP 1985

g. The responsiveness of the reaction force to the reported intrusion.

2. *Threat.* A careful evaluation of the threat posed to a particular secure area is a vital prerequisite to the formulation of an effective physical security plan for that area. The nature and degree of the threat vary widely with the geographical location and the operational environment; i.e., nonhostile or hostile. Variations in a nonhostile environment are primarily due to fluctuations of political or social unrest, economic factors, mobility of criminal elements, and changes in motivation at any given time. In a hostile environment, variations are due to the enemy's capabilities and tactics. On any installation, the threat to individual facilities varies because of the nature of the facility itself. The threat can be categorized as internal and external.

a. *Internal threat.* Personnel who work in, or have intimate knowledge of, the area and the security system form the source of the internal threat. This threat is generally considered to be a human reliability problem. Susceptibility to this threat can be reduced by incorporating certain security measures and procedures into hardware design, system installation, and system operation. For example, boxes, sensor covers, and cables can be designed to make them less vulnerable to tampering, and communication lines can be provided with tamper detection capability to prevent knowledgeable personnel from easily defeating the system.

b. *External threat.* The external threat can generally be described as follows:

(1) Intruders attempting penetration for the purpose of espionage, sabotage, conducting terrorist or paramilitary activity, theft for profit, and vandalism. Dissident groups or individuals who may be highly motivated and capable may try to reduce confidence in the military establishment, embarrass the Government, or create a dramatic incident to attract public attention. They could be expected to attempt entry without detailed planning or highly sophisticated equipment. They may evaluate the security posture by considering appropriate time factors, location vulnerability, and personnel and guard presence. They may attempt to bypass or otherwise defeat a detection system by covert means.

(2) Well-organized units can be expected to use overt force and diversionary actions to gain entry. Efficiency, depth of planning, execution, sophistication of equipment, and size of force may vary greatly. Alerting intelligence information will be necessary in

order to upgrade the defense or security posture required to effectively counter this threat.

3. *Classification.* Material of higher security classification should receive a higher degree of security than material of a lesser classification.

4. *Location.* The location of the secure area is a predominant consideration in determining the degree of security required. Some questions that may be addressed are the following: Are personnel on duty in the building 24 hours a day? Is the secure area part of a larger building? What are the entrance and exit routes? What is the degree of entry control? What is the response time of the reaction force?

5. *Construction:*

a. *General.* Four basic types of construction are addressed: (1) wood, (2) reinforced concrete, (3) nonreinforced concrete, and (4) masonry (brick, concrete block, etc.).

b. *Primary points of attack:*

(1) *Doors.* Doors constitute a primary point of intrusion. The intruder can be expected to attempt entry by cutting, breaking, or otherwise defeating the lock or hinges or by breaking through the door.

(2) *Alarm transmission lines.* A knowledgeable intruder is expected to first attempt to attack telephone or other transmission lines between the protected room and the monitoring area.

(3) *Walls, ceilings, floors.* A determined intruder can penetrate almost any type wall, ceiling, or floor in a matter of minutes with readily available tools.

(4) *Windows.* Windows, like doors, are a primary point of intrusion and are the hardest of all room features to protect.

(5) *Apertures.* Any rectangular opening having a minimum dimension greater than 6 inches with a cross-sectional area greater than 96 square inches, or any circular opening having a diameter greater than 10 inches, in walls, ceilings, floors, or doors must be considered as a possible point of entry.

(6) *Personnel.* Guards and personnel working within the secure area can be put under duress so that access to the secure area may be gained.

6. *Physical security.* Intrusion detection systems are not intended to replace physical security features such as locks, safes, et cetera. The number of levels of detection capability necessary is determined, in part, by the physical security aspects of the secure area.

16 SEP 1985

7. *Effectiveness.* The J-SIIDS was designed to be an effective, standardized, interior intrusion detection system for the Department of Defense. Its design characteristics are ease of installation and maintenance, ease of repair, and a minimal technical knowledge requirement on the part of the user. The system has a high detection capability and a low nuisance alarm susceptibility.

8. *Reaction force.* Once notice of an attempted intrusion has been given, the reaction force should be available to report to the scene in sufficient time to determine the nature of the alarm and take necessary action. Two important considerations are the following: (1) the time necessary for the intruder to complete his mission once he has been detected, and (2) the time necessary for the reaction force to arrive on the scene.

Part 2. System Description

0505. GENERAL

The Joint-Services Interior Intrusion Detection System (J-SIIDS) is designed to provide reliable detection on a 24-hour basis of intrusions, attempted intrusions, and equipment tampering attempts. All components of the J-SIIDS, except for the monitoring and display equipment, contain internal tamper switches that are activated when the component enclosure cover is removed or opened. All sensors requiring power are designed with a fail-safe mode whereby loss of power results in an alarm output. Primary power, 110 VAC to 125 VAC, 48 Hz to 62 Hz is required for the Control Unit and the Monitor Cabinets.

0506. J-SIIDS DESCRIPTION (BASIC SYSTEM).

1. The Joint-Services Interior Intrusion Detection System (fig. 5-1) consists of a family of intrusion and duress sensors, a control unit, monitoring and display equipment consisting of alarm and status monitor modules and monitor cabinets, a secure data transmission system, and an audible alarm. When properly

installed, the system functions to detect attempted and actual intrusions and notify the designated authorities.

2. The sensors and the control unit are located in the protected area. The control unit receives and processes the alarms from the sensors and supplies power to the sensors. The alarm and status signals, after processing, are relayed directly to the audible alarm, if used (except for a duress alarm) and to the monitor modules via the data transmission system or directly by unsupervised hardwire connections. The audible alarm normally is mounted on the outside of the room or building being protected and gives notice to personnel in the area that an alarm signal has been generated by the sensors. The monitoring and display equipment normally is located in an area where monitoring personnel are on duty 24 hours a day. The monitoring and display equipment consists of monitor cabinets and status or alarm monitor modules (one for each control unit). The status monitor module gives an audible and visual indication of alarm and status changes. The alarm monitor module only gives audible and visual indication of alarm conditions.

Part 3. J-SIIDS Components

0507. GENERAL

By using the J-SIIDS components that are described below, commands should be better able to select those types of alarm systems configurations that best suit their specific requirements.

0508. COMPONENTS

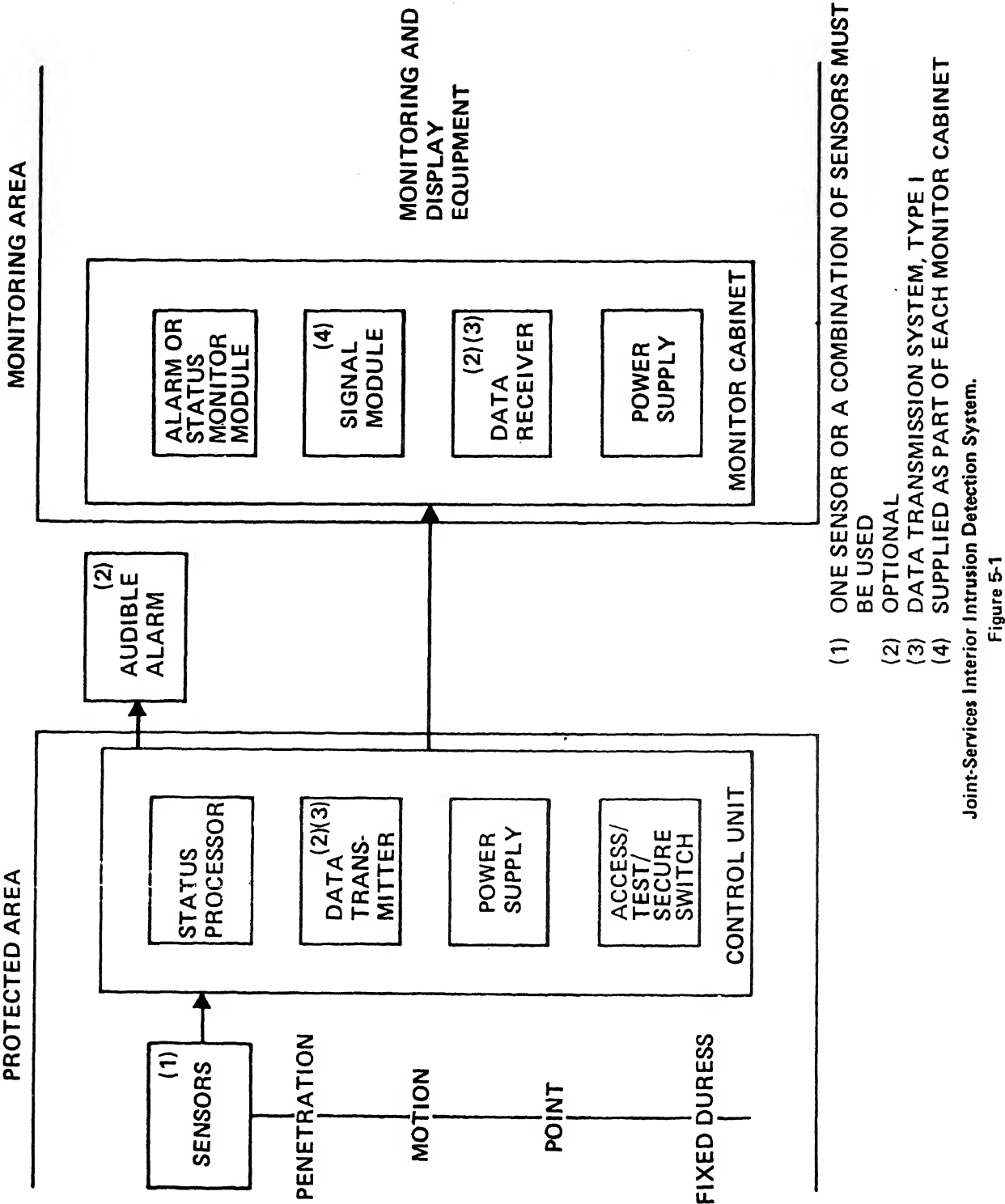
1. Control unit.

a. The control unit (CU) (fig. 5-2) is the central control element of the J-SIIDS and is located within

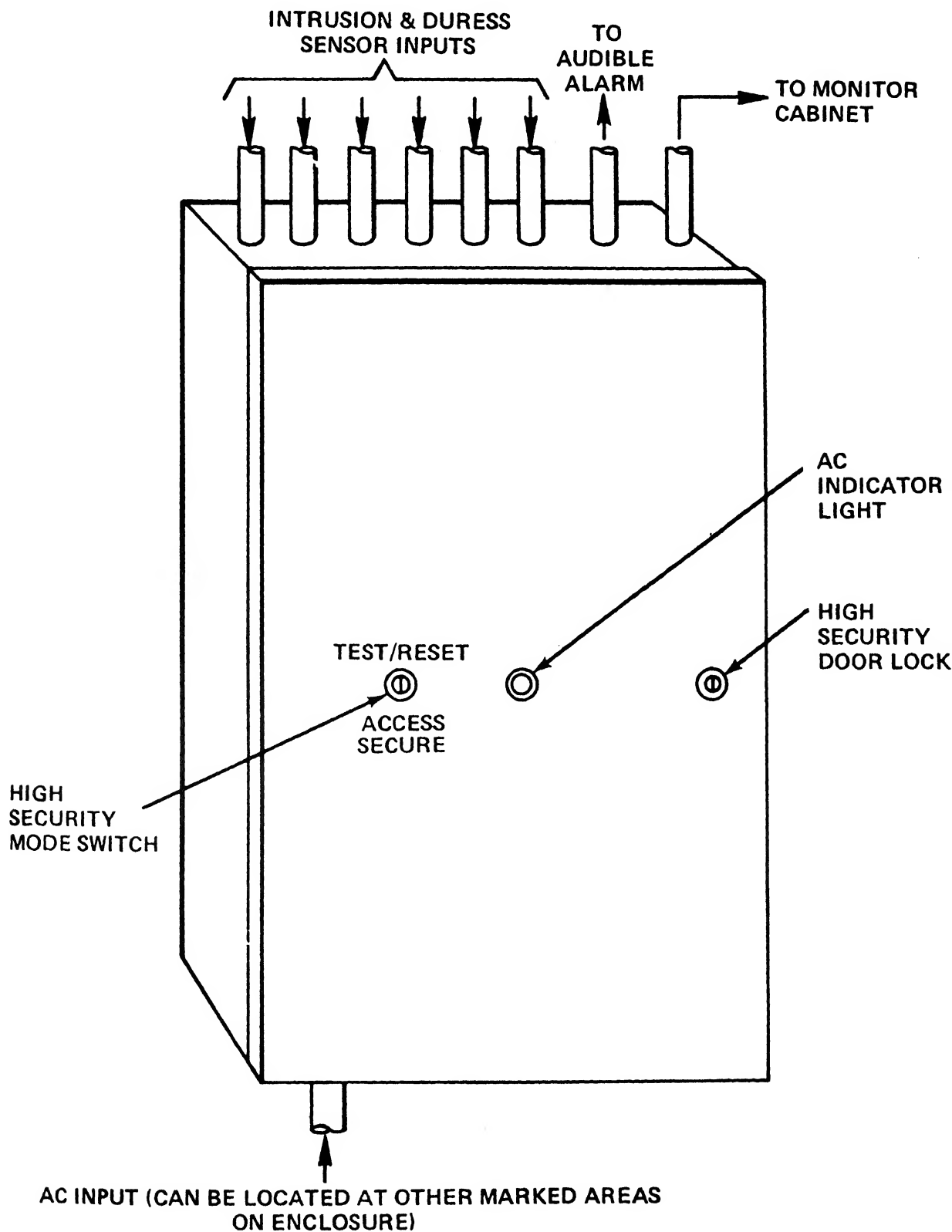
the protected area. It receives and processes the intrusion, tamper, and duress alarm signals generated at the sensors, provides for selection of the mode of operation (Access, Secure, Test/Reset) of the system, and continuously presents the status (Alarm, No Alarm) and mode of operation to the alarm monitor group.

b. The control unit contains an emergency standby (battery) power supply with an automatic switch-over which activates upon loss of primary AC power. Failure of power and switchover to emergency power

16 SEP 1985



16 SEP 1985



Control Unit
Figure 5-2

16 SEP 1985

is also presented to the monitor modules in the monitor cabinets.

c. The control unit is approximately 22¼ inches high by 14¼ inches wide by 8¼ inches deep and is mounted to the wall with four ¼ inch screws. Primary AC power requirements are 110 V to 125 V, 48 to 62 Hz, at 1.5 a.

d. The control unit has five intrusion sensor inputs plus a duress sensor input. This limitation does not affect the capability to use additional ultrasonic motion sensor, passive ultrasonic sensor, and vibration sensor transducers or multiple balanced magnetic switches or grid wire sensor sections on a single control unit intrusion sensor input.

e. The J-SIIDS mode of operation is key-switch selectable at the control unit. Three modes of operation are provided:

(1) Secure—The J-SIIDS is operated in the secure mode when the protected area is not open to authorized personnel. In this mode, all alarms are processed and presented to the monitor modules. All alarms except the duress alarm are presented to the audible alarm.

(2) Access—The J-SIIDS is operated in the access mode when the area is open to authorized personnel. In this mode all intrusion alarms are inhibited from being presented to either the monitor modules or the audible alarm. Tamper and duress alarms are presented to the alarm monitor and only tamper alarms are presented to the audible alarm.

(3) Test/Reset—In the third mode of J-SIIDS operation, Test/Reset, all alarms are inhibited from the audible alarm but are presented to the monitor modules and an audible sounding device is activated for 10 seconds at the control unit upon receipt of an alarm as an aid to J-SIIDS testing.

f. Some means of communication must be provided between the protected areas and the monitoring area to coordinate status changes.

2. Monitoring and display equipment.

a. General:

(1) The monitoring and display equipment (fig. 5-3) is the primary notification equipment of the J-SIIDS. It consists of monitor cabinets and one or more plug-in status monitor modules and/or alarm monitor modules. Three types or sizes of monitor cabinets are available; a single-zone with provisions for one plug-in monitor module, a five-zone with provisions for up to five monitor modules, and a 25-zone which accepts up to 25 monitor modules. Each type monitor cabinet has a self-contained signal module and primary and emergency (battery)

power supply. The signal module displays the status of the monitor cabinet power supply; i.e., operation on the primary or emergency source.

(2) The single-zone monitor cabinet is approximately 19 inches wide by 10½ inches high by 14 inches deep and is suitable for wall mounting with four ¼-inch screws or stacking on a flat surface such as a desk or table top. Primary AC power requirements are 110 V to 125 V, 48 Hz to 62 Hz, at 0.5 a.

(3) The five-zone monitor cabinet is approximately 33 1/2 inches wide by 21 1/8 inches high by 13 1/8 inches deep and is suitable for wall mounting with four 1/4-inch screws or stacking on a flat surface such as a desk or table top. Primary AC power requirements are 110 V to 125 V, 48 Hz to 62 Hz, at 1.0 a.

(4) The 25-zone monitor cabinet is approximately 24 inches wide by 57 inches high by 15 5/8 inches deep and is designed to be free standing on the floor. Primary AC power requirements are 110 V to 125 V, 48 Hz to 62 Hz, at 5.0 a.

(5) Each monitor cabinet contains an emergency standby (battery) power supply with automatic switchover which activates upon loss of primary AC power. The emergency supply is sufficient for 24 hours of operation for the single-zone cabinet, 20 hours of operation for the five-zone cabinet, and 12 hours of operation for the 25-zone cabinet.

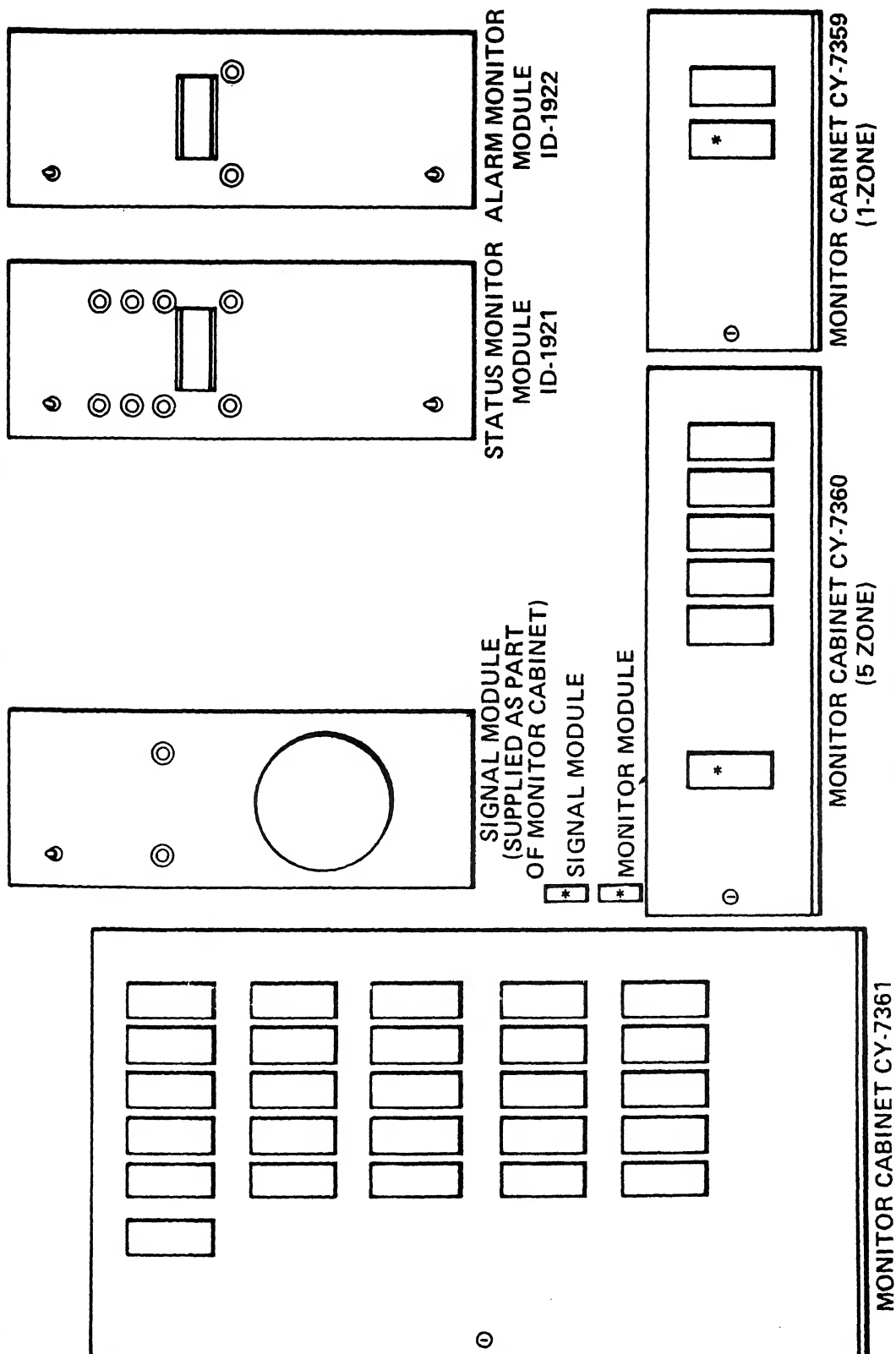
(6) The monitor cabinets and monitor modules interface directly with the control unit via unsupervised, hard-wired interconnecting wiring or via a data transmission system over a twisted wire pair or dedicated telephone lines. The unsupervised interconnection is used only when the control unit and the monitoring and display equipment are within the same building and the interconnecting wiring is enclosed in conduit.

(7) The plug-in monitor modules (status or alarm) interface directly with individual control units. The status of the secured areas (alarm, no alarm, AC on, AC fail) and mode of operation (access, secure), as processed by the control units, is continuously displayed on the status monitor module, whereas only the status (alarm, no alarm) is displayed on the alarm monitor module.

b. Status monitor module:

(1) All status monitor modules within the monitor cabinets are identical and each displays the status and mode of operation of one control unit. The six different status and mode of operation conditions (secure, access, alarm, no alarm, AC on, AC fail) are displayed by means of four pairs of status lights labeled "secure," "access," "AC power," and

16 SEP 1985



Components of Monitoring and Display Equipment.

Figure 5-3

16 SEP 1985

is also presented to the monitor modules in the monitor cabinets.

c. The control unit is approximately 22¼ inches high by 14¼ inches wide by 8¼ inches deep and is mounted to the wall with four ¼ inch screws. Primary AC power requirements are 110 V to 125 V, 48 to 62 Hz, at 1.5 a.

d. The control unit has five intrusion sensor inputs plus a duress sensor input. This limitation does not affect the capability to use additional ultrasonic motion sensor, passive ultrasonic sensor, and vibration sensor transducers or multiple balanced magnetic switches or grid wire sensor sections on a single control unit intrusion sensor input.

e. The J-SIIDS mode of operation is key-switch selectable at the control unit. Three modes of operation are provided:

(1) Secure—The J-SIIDS is operated in the secure mode when the protected area is not open to authorized personnel. In this mode, all alarms are processed and presented to the monitor modules. All alarms except the duress alarm are presented to the audible alarm.

(2) Access—The J-SIIDS is operated in the access mode when the area is open to authorized personnel. In this mode all intrusion alarms are inhibited from being presented to either the monitor modules or the audible alarm. Tamper and duress alarms are presented to the alarm monitor and only tamper alarms are presented to the audible alarm.

(3) Test/Reset—In the third mode of J-SIIDS operation, Test/Reset, all alarms are inhibited from the audible alarm but are presented to the monitor modules and an audible sounding device is activated for 10 seconds at the control unit upon receipt of an alarm as an aid to J-SIIDS testing.

f. Some means of communication must be provided between the protected areas and the monitoring area to coordinate status changes.

2. Monitoring and display equipment.

a. General:

(1) The monitoring and display equipment (fig. 5-3) is the primary notification equipment of the J-SIIDS. It consists of monitor cabinets and one or more plug-in status monitor modules and/or alarm monitor modules. Three types or sizes of monitor cabinets are available; a single-zone with provisions for one plug-in monitor module, a five-zone with provisions for up to five monitor modules, and a 25-zone which accepts up to 25 monitor modules. Each type monitor cabinet has a self-contained signal module and primary and emergency (battery)

power supply. The signal module displays the status of the monitor cabinet power supply; i.e., operation on the primary or emergency source.

(2) The single-zone monitor cabinet is approximately 19 inches wide by 10½ inches high by 14 inches deep and is suitable for wall mounting with four ¼-inch screws or stacking on a flat surface such as a desk or table top. Primary AC power requirements are 110 V to 125 V, 48 Hz to 62 Hz, at 0.5 a.

(3) The five-zone monitor cabinet is approximately 33 1/2 inches wide by 21 1/8 inches high by 13 1/8 inches deep and is suitable for wall mounting with four 1/4-inch screws or stacking on a flat surface such as a desk or table top. Primary AC power requirements are 110 V to 125 V, 48 Hz to 62 Hz, at 1.0 a.

(4) The 25-zone monitor cabinet is approximately 24 inches wide by 57 inches high by 15 5/8 inches deep and is designed to be free standing on the floor. Primary AC power requirements are 110 V to 125 V, 48 Hz to 62 Hz, at 5.0 a.

(5) Each monitor cabinet contains an emergency standby (battery) power supply with automatic switchover which activates upon loss of primary AC power. The emergency supply is sufficient for 24 hours of operation for the single-zone cabinet, 20 hours of operation for the five-zone cabinet, and 12 hours of operation for the 25-zone cabinet.

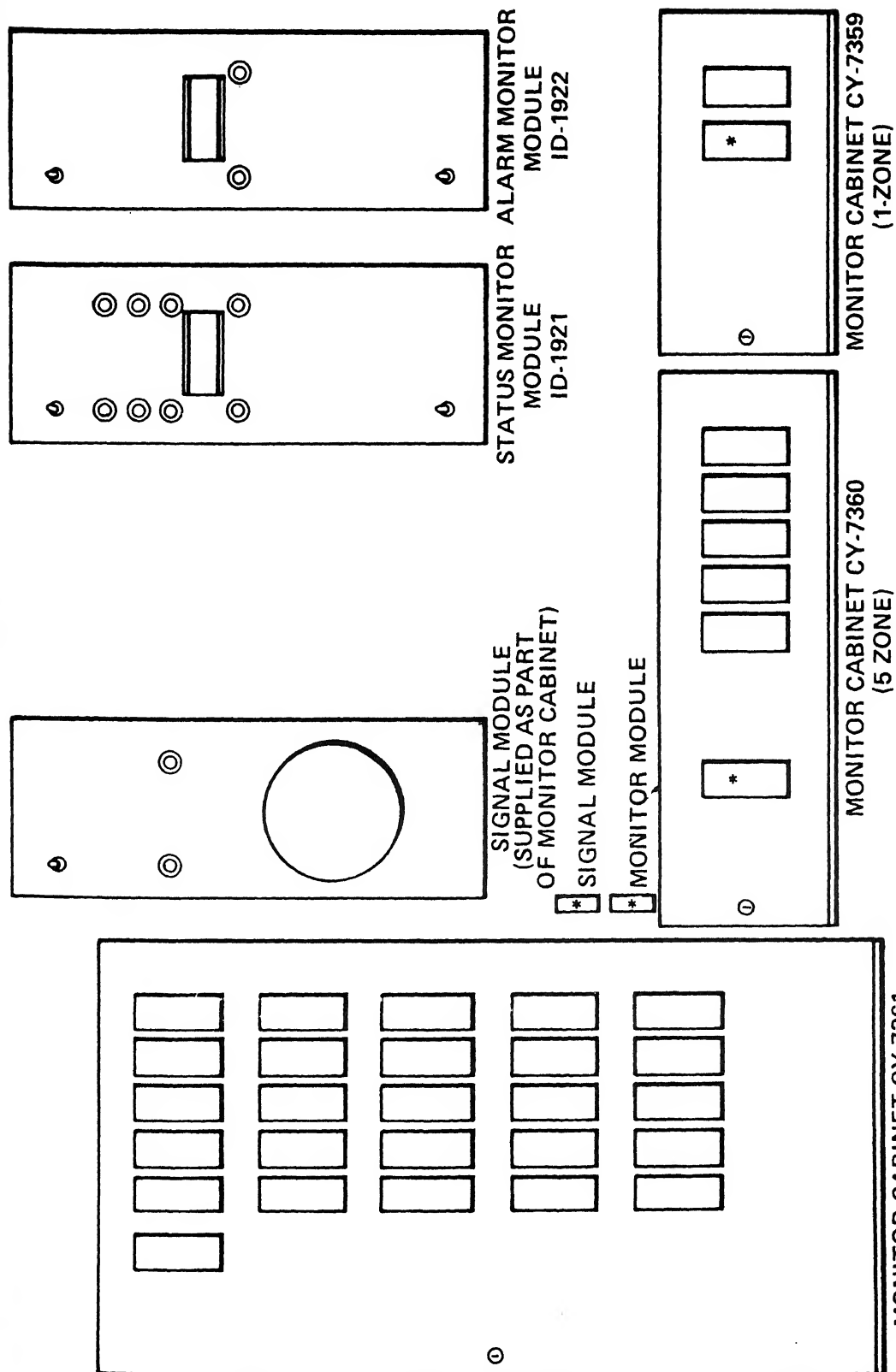
(6) The monitor cabinets and monitor modules interface directly with the control unit via unsupervised, hard-wired interconnecting wiring or via a data transmission system over a twisted wire pair or dedicated telephone lines. The unsupervised interconnection is used only when the control unit and the monitoring and display equipment are within the same building and the interconnecting wiring is enclosed in conduit.

(7) The plug-in monitor modules (status or alarm) interface directly with individual control units. The status of the secured areas (alarm, no alarm, AC on, AC fail) and mode of operation (access, secure), as processed by the control units, is continuously displayed on the status monitor module, whereas only the status (alarm, no alarm) is displayed on the alarm monitor module.

b. Status monitor module:

(1) All status monitor modules within the monitor cabinets are identical and each displays the status and mode of operation of one control unit. The six different status and mode of operation conditions (secure, access, alarm, no alarm, AC on, AC fail) are displayed by means of four pairs of status lights labeled "secure," "access," "AC power," and

16 SEP 1985



Components of Monitoring and Display Equipment.

Figure 5-3

16 SEP 1985

"alarm." The no-alarm condition is indicated by the absence of the alarm lights and the AC fail condition is indicated by the absence of the AC power lights.

(2) Each change of status from one state to the corresponding opposite state is accompanied by the flashing light associated with the new state and the sounding of an audible signal (located in the monitor cabinet common signal module) until the "acknowledge" switch is momentarily depressed. When this switch is depressed, the flashing light associated with the new state changes to a continuously illuminated light (except for the AC fail and the no alarm status conditions) and the audible signal is silenced.

(3) The status monitor modules interface with the monitor cabinets by means of plug-in connectors. The modules have an additional connector for interfacing with the data transmission system receiver when the data transmission system is used between the control unit and the monitoring and display equipment. The receiver plugs into the monitor module.

c. Alarm monitor module. The alarm monitor module is used in the monitor cabinets when it is desired that only alarm information be displayed. The alarm monitor modules are completely interchangeable with the status monitor modules.

3. Data transmission system (type I).

a. The data transmission system (DTS), illustrated in figure 5-4 is used to provide secure transmissions between the control unit, located in the secured area, and the monitoring and display equipment, normally located some distance from the secured area. The data transmission system consists of a data transmitter mounted within the control unit and a data receiver connected to a monitor module located within the monitor cabinet.

b. The data transmission system is designed to operate over a maximum of 10 miles of 600-ohm, 2-wire, balanced transmission line or over telephone systems using dedicated voice-grade lines. The data transmission system is used whenever there are segments of the transmission line that are open or accessible to tampering. In those cases where the transmission line can be provided with complete end-to-end physical protection; e.g., where the line is enclosed in rigid conduit and within a building, the data transmission system may not be required and the control unit and monitoring equipment can be directly connected, but with degradation in line security and a complete loss of line supervision.

c. The data transmission system continuously monitors the status and mode of operation of the

secured area, as processed by the control unit. This information is encoded prior to transmission. Secure signal transmission is achieved through the use of synchronized pseudorandom binary sequence generators in the transmitter and receiver. Synchronization of these generators is automatic upon application of DC power to the transmitter. They can also be manually synchronized by momentary activation of a switch located within the control unit.

d. The data transmission system has been designed to preclude the possibility of nuisance alarms and transmission of incorrect data caused by degradation (noise, momentary dropouts, line loading) of the transmission media. The transmission line is also continuously monitored for indications of tampering and other attempts at compromise.

4. Audible alarm.

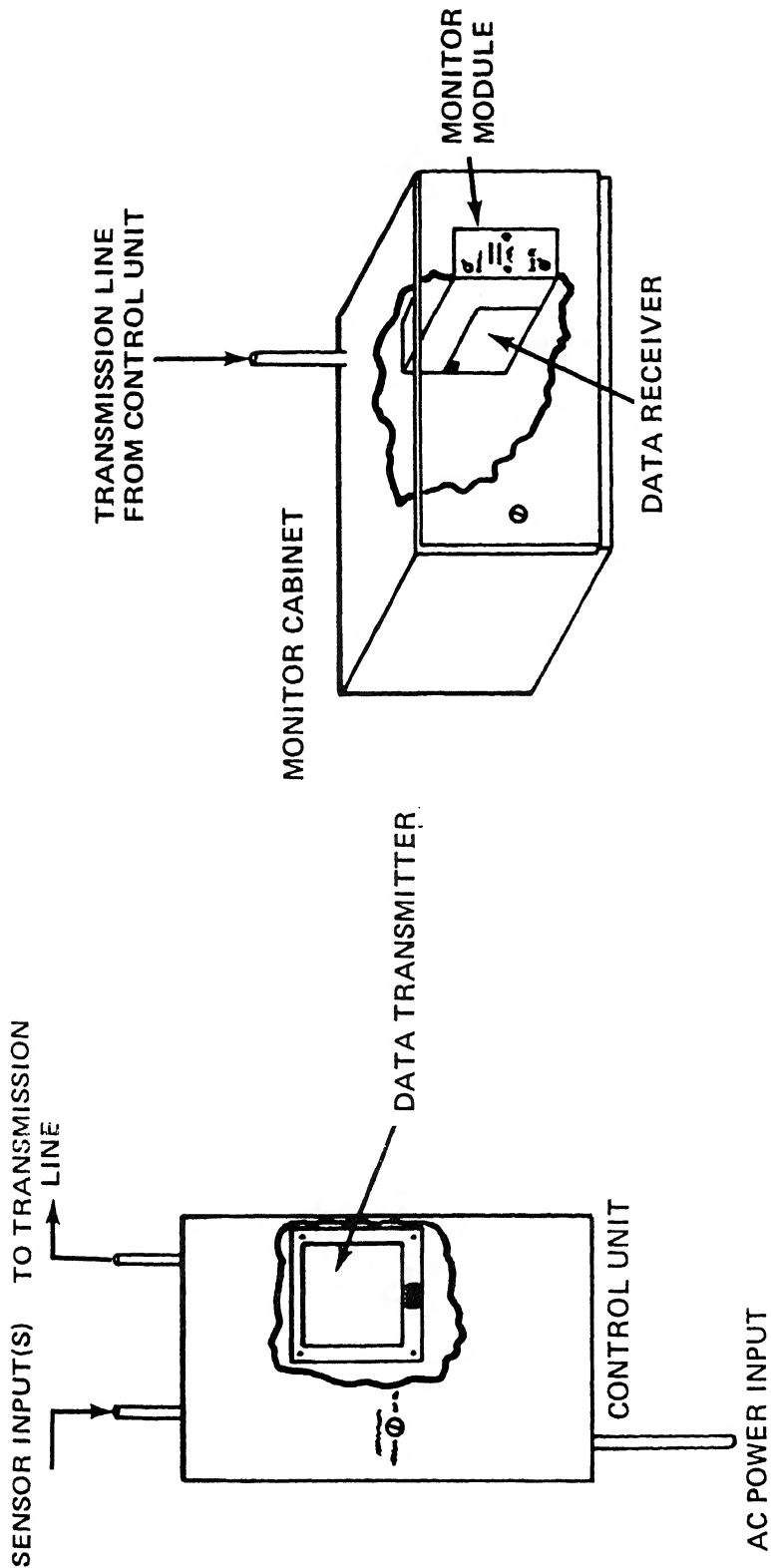
a. The audible alarm (fig. 5-5) is used when a loud audible alarm signal is desired to alert personnel in the immediate vicinity to an intrusion or tamper alarm condition. The audible alarm interfaces directly by hardwire to the control unit and normally is mounted to an exterior wall in the near vicinity of the secured area. Only one control unit may be connected to a single audible alarm. The audible alarm is not activated when an alarm is initiated by the latching alarm switch (duress sensor). This feature is intended to afford protection to duty personnel placed under duress, since the audible alarm activation would alert the intruder that an alarm had been initiated.

b. The audible alarm is approximately 12 inches wide by 15 inches high by 6 inches deep. Primary AC power to the audible alarm is provided through the control unit. A separate source of AC power is not required. Emergency power is self-contained and is sufficient to provide for alarm sounding at a level of 110 dB for a minimum period of 15 minutes.

c. Since the audible alarm is mounted externally to the building within which the secured area is located, it is relatively vulnerable to attempts at compromise. Tamper protection is provided through the use of pry-off tamper switches which cause an alarm to be activated when the enclosure is removed from the mounting surface. Enclosure door tamper switches cause an alarm to be activated when the enclosure door is opened. A double enclosure, one within the other, causes an alarm to be activated when the enclosures are shorted together, as would occur during attempts to drill through the enclosures.

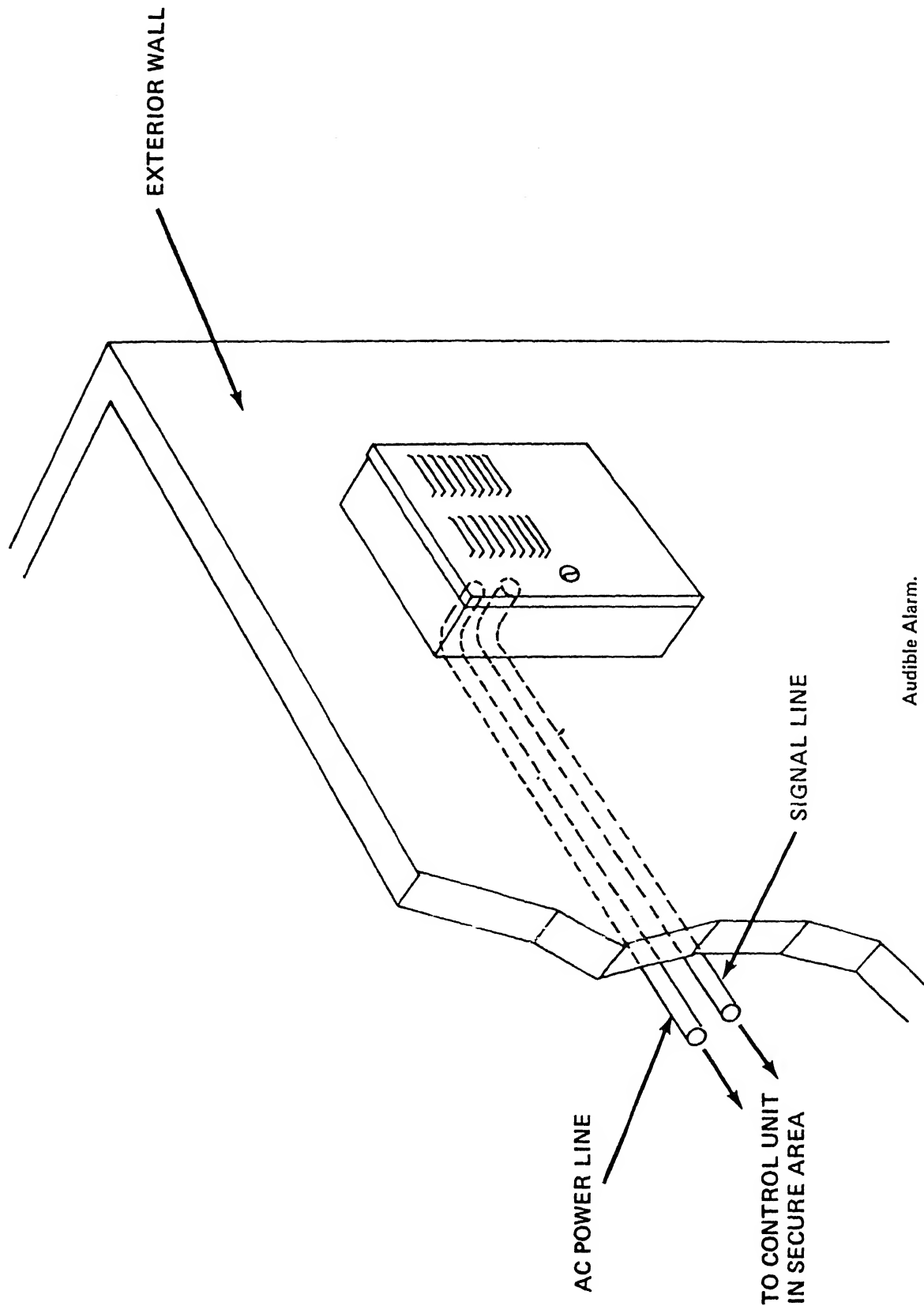
d. The alarm can be heard at distances of approximately 500 feet.

16 SEP 1985



Data Transmission System.

Figure 5-4



Audible Alarm.
Figure 5-5

16 SEP 1985

5. Sensor components.

a. *General.* The various sensors available as J-SIIDS components are classified as follows:

(1) Penetration sensors—those designed to detect penetration into the protected area, including entry through doors, windows, walls, floors, ceiling, and other openings in the room.

(2) Motion sensors—those designed to detect movement of a person within the protected area.

(3) Point sensors—those designed to detect the attempted removal of an item from its normal position within the protected area.

(4) Duress sensors—those designed to be activated by guard personnel to call for assistance under situations of duress.

b. Penetration sensors:

(1) *Balanced magnetic switch* (fig. 5-6). The balanced magnetic switch (BMS) is a magnetically operated switch used to detect the opening of a secured door (or window). It consists of a switch assembly and an actuating magnet assembly. The switch assembly is 4 3/4 inches long by 2 1/2 inches wide by 1 1/2 inches long by 7/8 inches wide by 1 1/2 inches deep. The actuating magnet assembly is 4 1/2 inches long by 7/8 inches wide by 1 1/2 inches deep. The switch assembly mounts on the inside of the door frame, and the actuating magnet mounts on the door as shown in figure 5-6. When the door (or window) is closed, the field from the actuating magnet interacts with a second field inside the switch assembly to balance the magnetic field and allow the switch to close. When the (secured) door (or window) is opened the actuating magnet is moved away from the switch assembly, the field inside the switch assembly becomes unbalanced and forces the switch to open, and an intrusion alarm is signaled. With the door closed, any change in the external field, either by the addition of an external magnet to the outside of the switch assembly case, or by the insertion of a shield between the switch assembly and the actuating magnet, will disturb the balance, cause the switch to open, and initiate an alarm.

(2) *Capacitance proximity sensor* (fig. 5-7):

(a) The capacitance proximity sensor (GPS) is designed to detect penetration through windows, ventilators, and other similar openings. The sensor may also be used as a point sensor as described in paragraph 5(d) below. The sensor continually monitors the net capacitance between sensor protected metal objects and a reference ground. When used as a penetration sensor, the metal objects consist of metal

grills which are insulated from ground and mounted over the openings.

NOTE

The grills are fabricated locally out of any conducting material (e.g., metal fencing material or expanded metal) and are not supplied as part of the sensor.

(b) When an intruder approaches or touches the metal grill, the capacitance between the grill and ground is changed. This change in capacitance is sensed by the signal processor, and an alarm is generated. The sensor is designed such that slowly changing capacitance caused by normal changes in environmental conditions will not cause an alarm to be generated. Operating power is supplied by the control unit.

(c) The items furnished as part of the capacitance proximity sensor are a signal processor in an enclosure approximately 6 X 6 X 4 inches and 50 feet of RG 58/U coaxial cable.

(3) *Grid wire sensor* (fig. 5-8):

(a) The grid wire sensor (GWS) is used to detect forced entry through walls, floors, ceiling, doors, windows, and other barriers. The surface of the barrier is covered by a continuous wire in a 4-inch-square grid pattern. Fire-resistant wood panels are then installed over the wire grid to protect the grid from day-to-day abuse and to hide the exact location of the grid. Any penetration or attempted penetration of the barrier larger than the 4-inch square breaks the wire at one or more points and causes an intrusion alarm to be generated.

(b) Use of wooden materials for the foundation board of the grid wire sensor is contingent upon availability of fire-resistive materials and compliance with appropriate fire prevention criteria.

(c) The grid wire sensor is supplied in a kit containing all the material required for installation of the sensor. Each kit contains the following:

Grid wire: 600 feet

Grid wire enclosure (5 inches long X 4 1/2 inches wide X 2 inches deep): 1

Grid wire connectors: 4

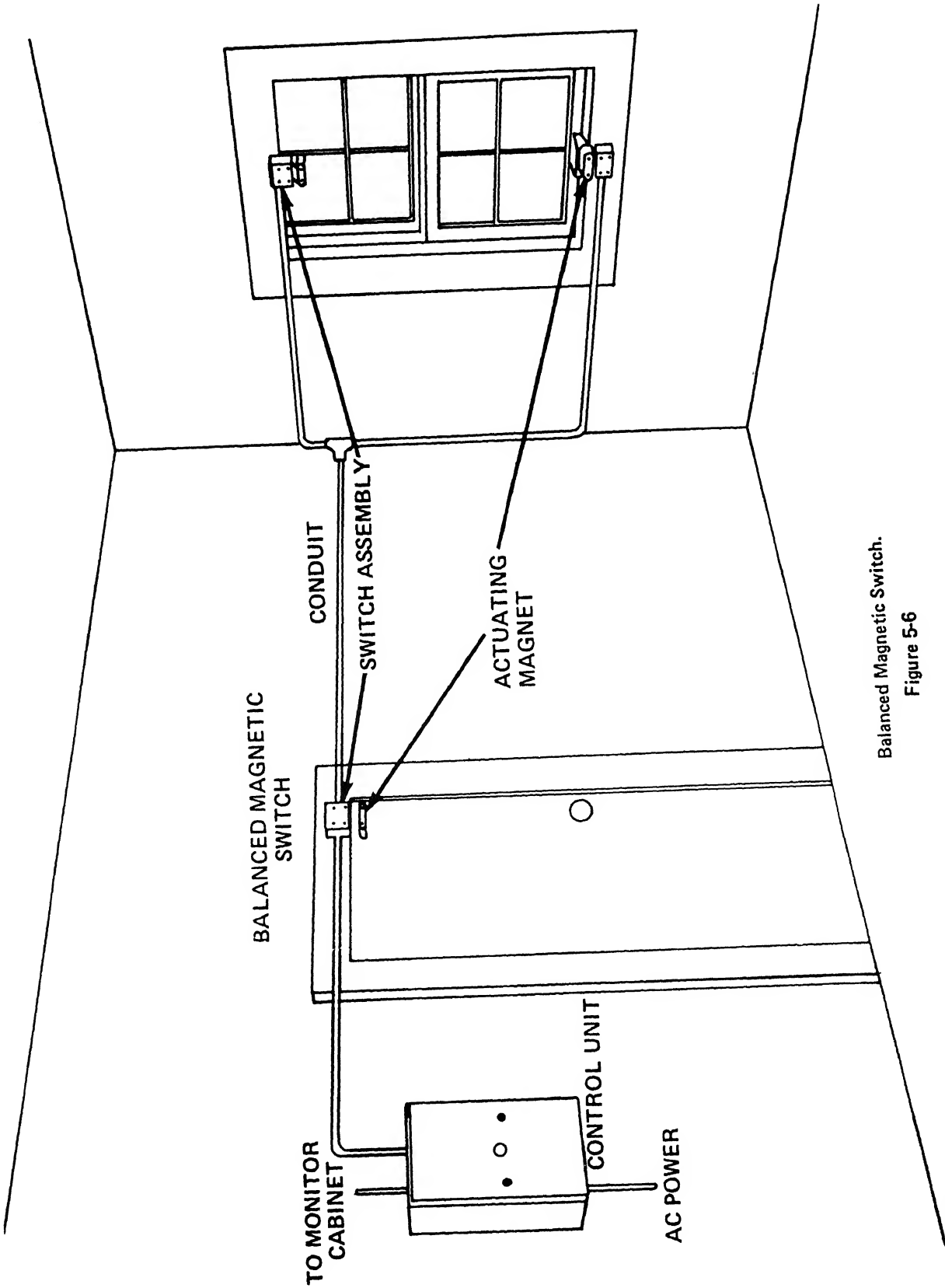
Connector crimping tool: 1

Grid wire application device (staple): 1

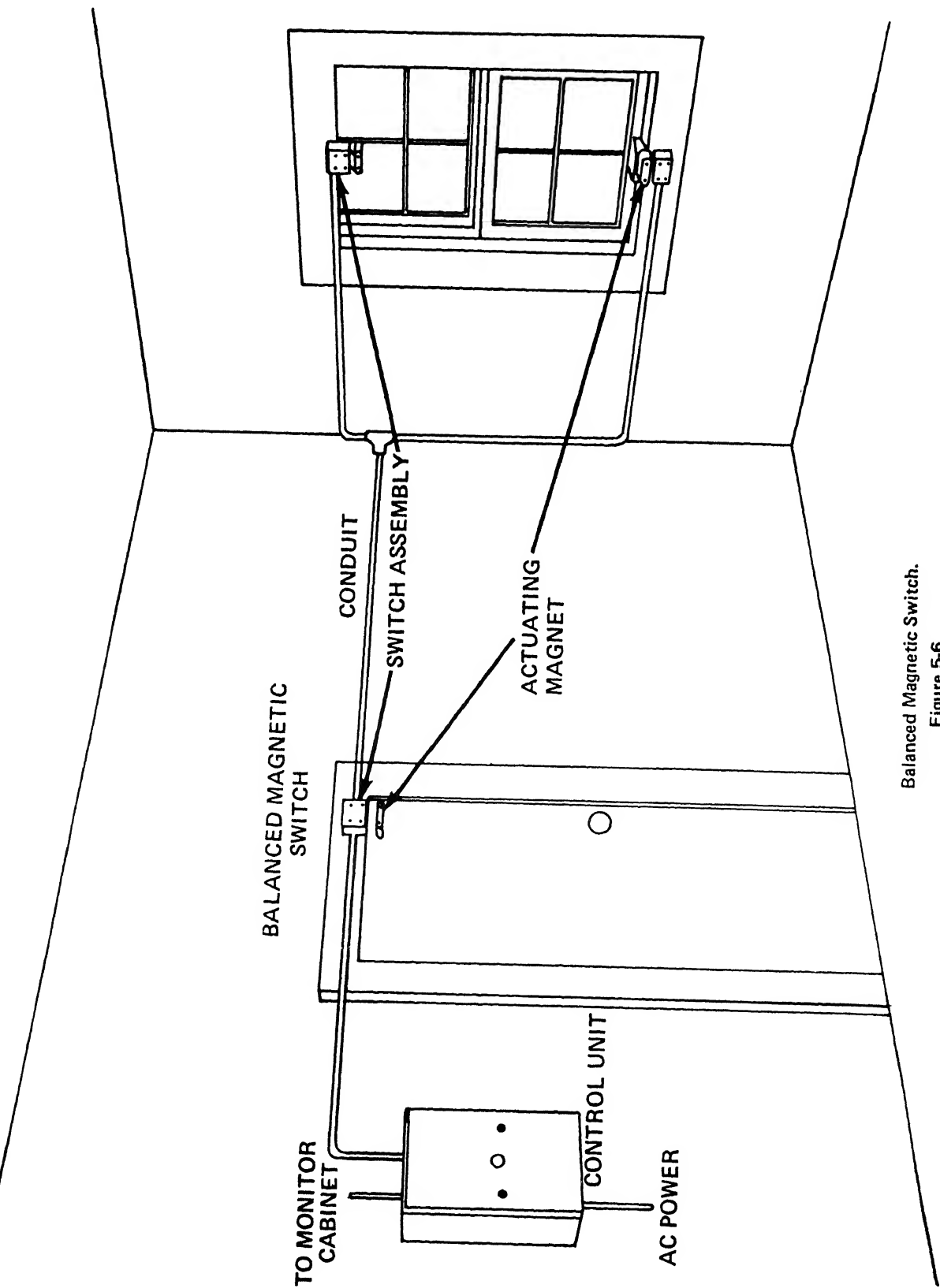
Staples: 1,000

Each kit has sufficient material to cover an area of approximately 160 square feet.

(d) If the barrier to which the wire grid is to be attached is not suitable for stapling, e.g., concrete,

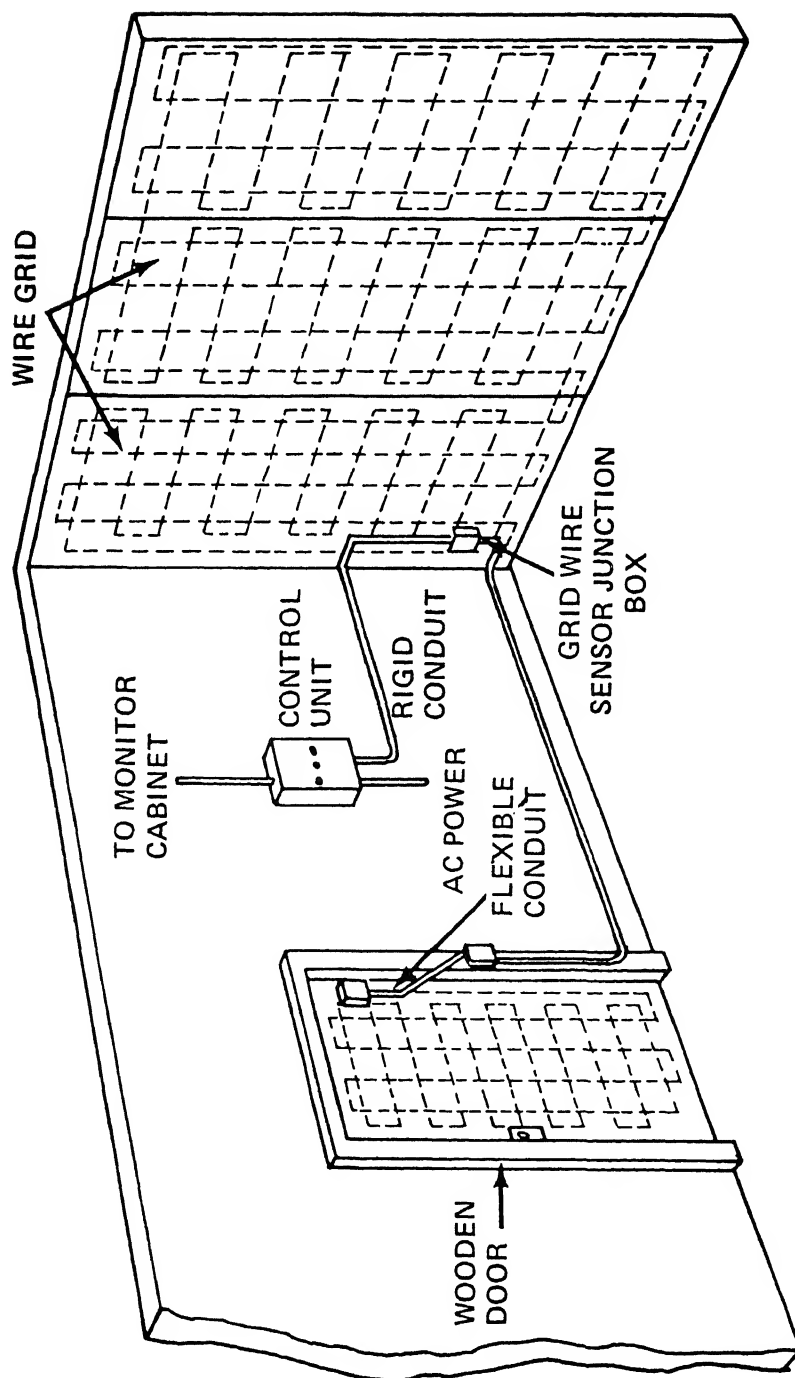


Balanced Magnetic Switch.
Figure 5-6



Balanced Magnetic Switch.
Figure 5-6

6 SEP 1985



Grid Wire Sensor.

Figure 5-8

16 SEP 1985

cinder block, or plaster, the wire grid should be applied to a fire-resistant foundation board of plywood which has been securely fastened to the barrier.

(4) *Vibration sensor* (fig. 5-9). The vibration sensor (VS) is designed to protect against forced entry through expanded metal room liners and metal barriers placed over windows and other openings in the protected area. The sensor detects structurally transmitted vibrations imposed on the metal barrier by sawing, drilling, and other similar penetration attempts and generates an alarm when the energy generated satisfies certain design criteria. The sensor consists of a signal processor and multiple vibration detectors. Detectors are not provided with the signal processor. The detectors must be ordered separately. The signal processor is approximately 9 inches long by 10 inches wide by $2\frac{1}{16}$ inches deep. The detectors are approximately $5\frac{3}{4}$ inches long by $4\frac{3}{4}$ inches wide by $2\frac{1}{8}$ inches deep. Up to 20 vibration detectors can be connected to one signal processor. Each detector is designed to detect vibrations caused by penetration attempts within a radius of 4 feet from the detector. Operating power is supplied by the control unit.

(5) *Passive ultrasonic sensor* (fig. 5-10):

(a) The passive ultrasonic sensor (PUS) is designed to protect against forced entry through metal and masonry walls, ceilings, and floors and through metal doors, metal mesh, and barred or shuttered windows and ventilation openings when these openings are properly sealed against outside sounds. The sensor detects repetitive ultrasonic energy that is generated when a penetration is attempted through these barriers by sawing, hammering, drilling, or burning with a torch, and alarms when the energy generated satisfies certain design criteria.

(b) The passive ultrasonic sensor can also be used to protect against forced entry through wooden walls, when these walls are sealed against outside sounds and when this sensor is used in conjunction with the ultrasonic motion sensor. The ultrasonic motion sensor provides backup to the passive ultrasonic sensor in case penetration through the wooden walls is achieved without creating sufficient ultrasonic energy to activate the passive ultrasonic sensor and also provides perimeter protection in that the initial breakthrough or motion through the wall will be detected.

(c) The sensor consists of a signal processor and multiple ultrasonic receivers. The receivers are not provided with the signal processor and must be ordered separately. The signal processor is approxi-

mately 5 inches long by 10 inches wide by $2\frac{1}{16}$ inches deep. The receivers are approximately $5\frac{3}{4}$ inches long by $4\frac{3}{4}$ inches wide by $2\frac{1}{8}$ inches deep. Up to 20 receivers can be connected to one signal processor to achieve large area coverage. Each receiver is designed to detect ultrasonic energy at a level in excess of normal background levels between 50 and 80 dB in an area having a floor space of approximately 20×15 feet. In order to achieve coverage of all four walls, a minimum of two receivers must be used, preferably located in opposite corners, as shown in figure 5-10. Operating power is supplied by the control unit.

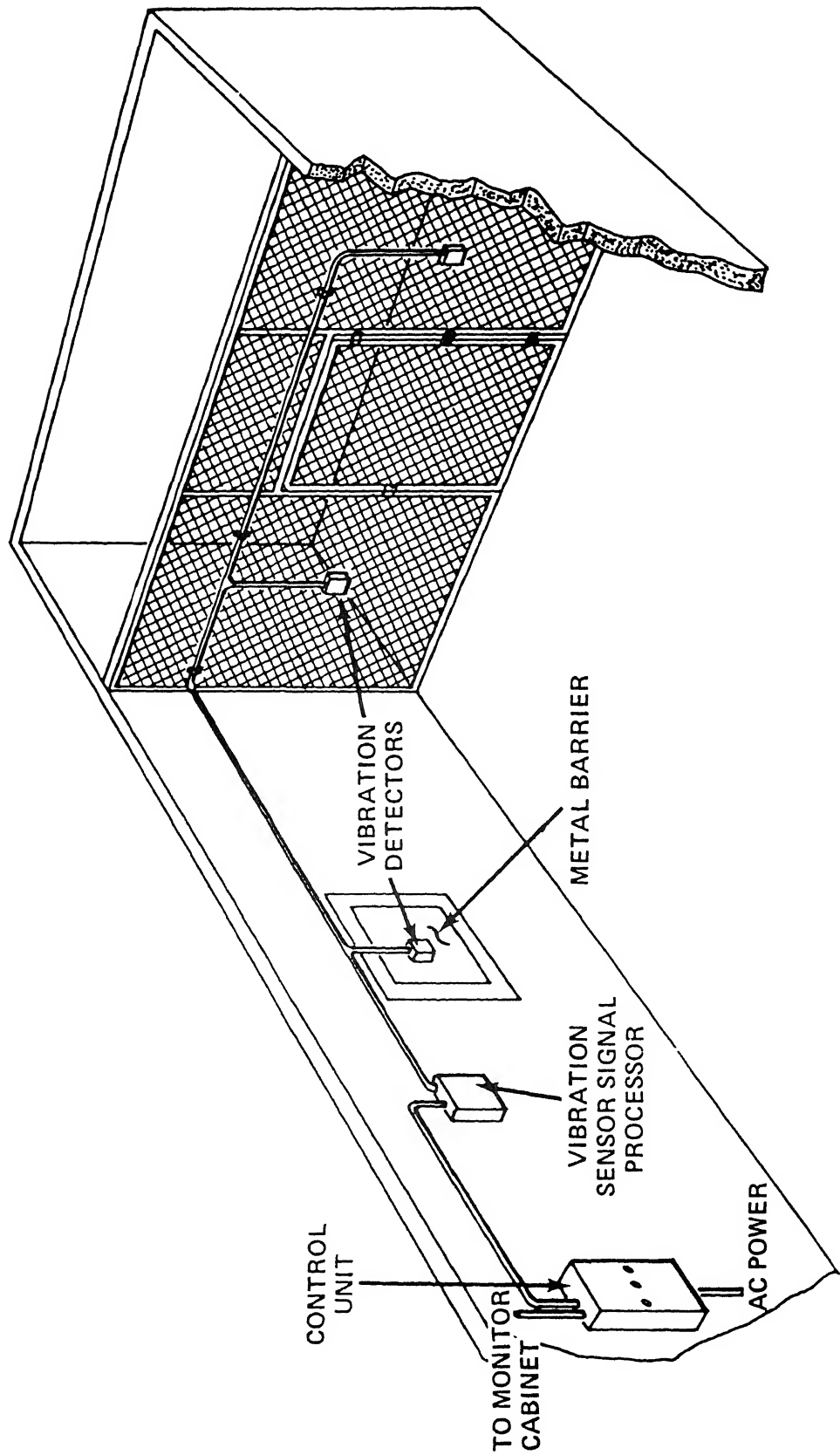
c. *Ultrasonic motion sensor:*

(1) The ultrasonic motion sensor (UMS) (fig. 5-11) detects the motion of an intruder inside the protected area. The sensor detects the Doppler frequency shift of the received ultrasonic signal caused by radial components of the intruder's motion. A transmitter transducer radiates an ultrasonic signal which is reflected from the surfaces within the protected room. A receiving transducer receives the reflected signals. The reflected signal is compared to the transmitted signal in the signal processor. If no relative motion exists within the protected room, the received and transmitted signals are at the same frequency. Radial motion components, however, cause the received signal to differ in frequency from the transmitted signal. The signal processor detects this frequency change (Doppler shift) and initiates an alarm condition when certain design criteria have been met. The sensor is designed to recognize and discriminate against air turbulence, blowing curtains, vibrating walls, and similar nuisance alarm creating phenomena.

(2) The sensor consists of a signal processor and multiple ultrasonic transceivers. The transceivers are not provided with the signal processor and must be ordered separately. The signal processor is approximately 5 inches wide by 10 inches long by $2\frac{1}{16}$ inches deep. The transceiver is approximately 19 inches high by $3\frac{3}{4}$ inches wide by $2\frac{3}{4}$ inches deep. Up to 20 transceivers can be connected to one signal processor to achieve large area coverage. Each transceiver is designed to provide coverage over a floor area of approximately 30×20 feet except as noted in figure 5-14. Operating power is supplied by the control unit.

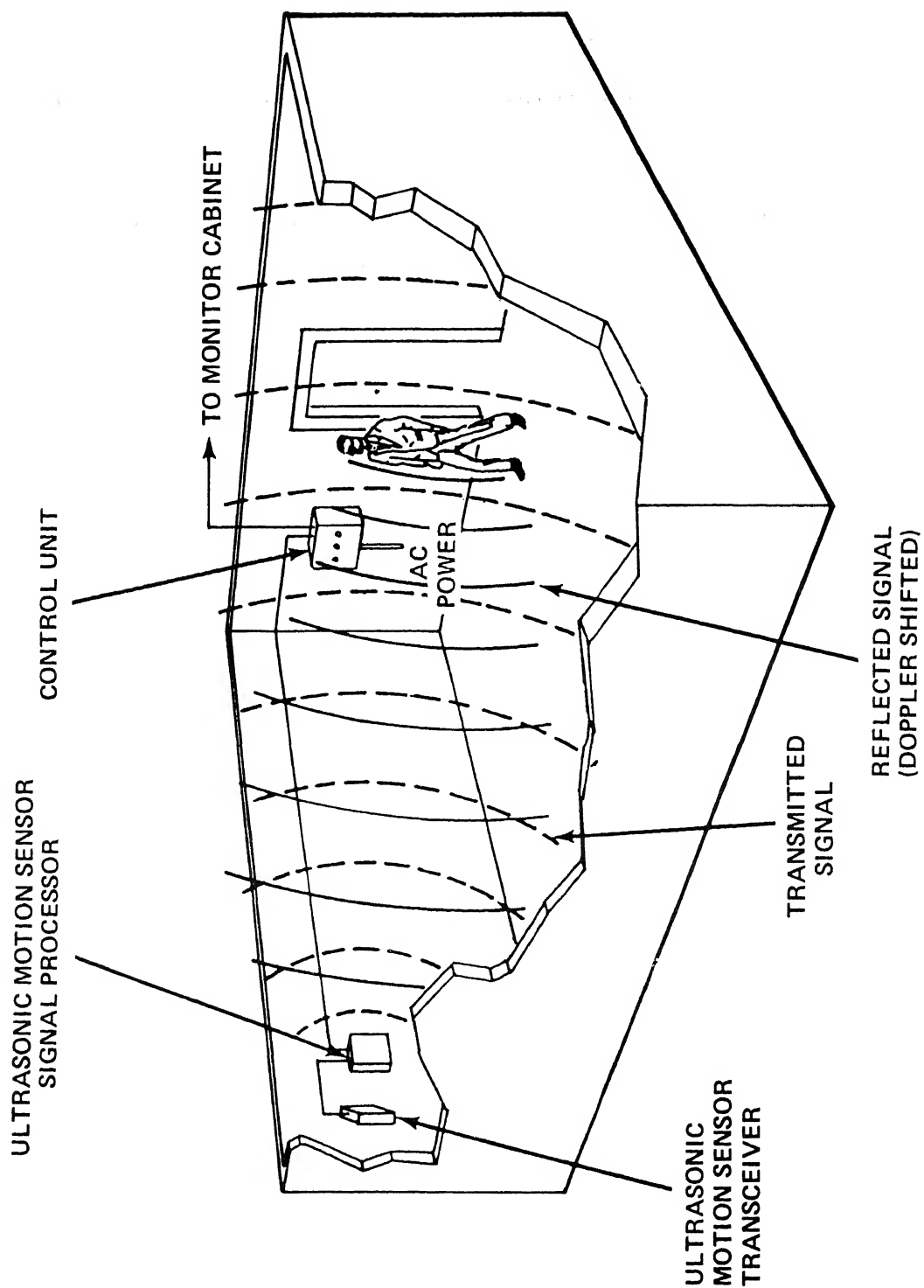
d. *Point sensors.* The capacitance proximity sensor can be used as a point sensor. When used as a point sensor, it is used to protect metal containers

16 SEP 1985



Vibration Sensor.
Figure 5-9

16 SEP 1985



Ultrasonic Motion Sensor.

Figure 5-11

16 SEP 1985

such as safes and file cabinets. The sensor initiates an alarm when a hand or tool is brought within close proximity of the container or upon actual contact with the container. The container must be insulated from the floor. Unless rugs, carpets, et cetera, provide sufficient insulation, insulating blocks must be used. The insulating blocks are not supplied with the sensor and must be ordered separately.

e. Duress sensor (latching alarm switch) (fig. 5-12). This sensor is a holdup notification device. It is used by personnel to manually initiate a duress alarm. It can be mounted to the wall or floor in close proximity to personnel stations and can be hand or foot operated. Operating power is supplied by the control unit. The latching alarm switch does not cause activation of the audible alarm.

Part 4. Component Selection and Application

0509. GENERAL

In-depth security can be achieved by equipping the secure area with a minimum of two levels of detection capability chosen from the following three:

1. *Penetration detection.* Detection of penetration attempts into the secure area includes entry through doors, windows, walls, floors, ceiling, and any other openings in the room.

2. *Motion detection.* Detection of movement of a person inside the secure area.

3. *Point detection.* Detection of attempts at removal of protected items inside the secure area.

0510. PENETRATION DETECTION

This outermost level of detection capability, the "early warning," is the level that should be applied with the most thorough and painstaking planning. When a particular secure area is to be fitted with penetration detection components, care must be taken to insure the entire perimeter of the secure area (including windows, ceiling, and floors) is penetration protected. A thorough evaluation of the structure should be made to identify all possible points of attack.

1. Doors.

- a. General.* Doors constitute a primary point of intrusion through the boundaries of the secured area. The intruder can be expected to attempt entry through a door by cutting or breaking the lock or by breaking through the door. Doors need to be monitored for unauthorized opening and for breakthrough. The balanced magnetic switch is used to detect the opening of a door. Breakthrough detection is achieved by use of either the passive ultrasonic sensor, the vibration sensor, or the grid wire sensor. The balanced magnetic switch should be mounted on the inside of the doors leading into the secured area unless unique circumstances dictate otherwise. Locating the switch on the outside of the door makes the

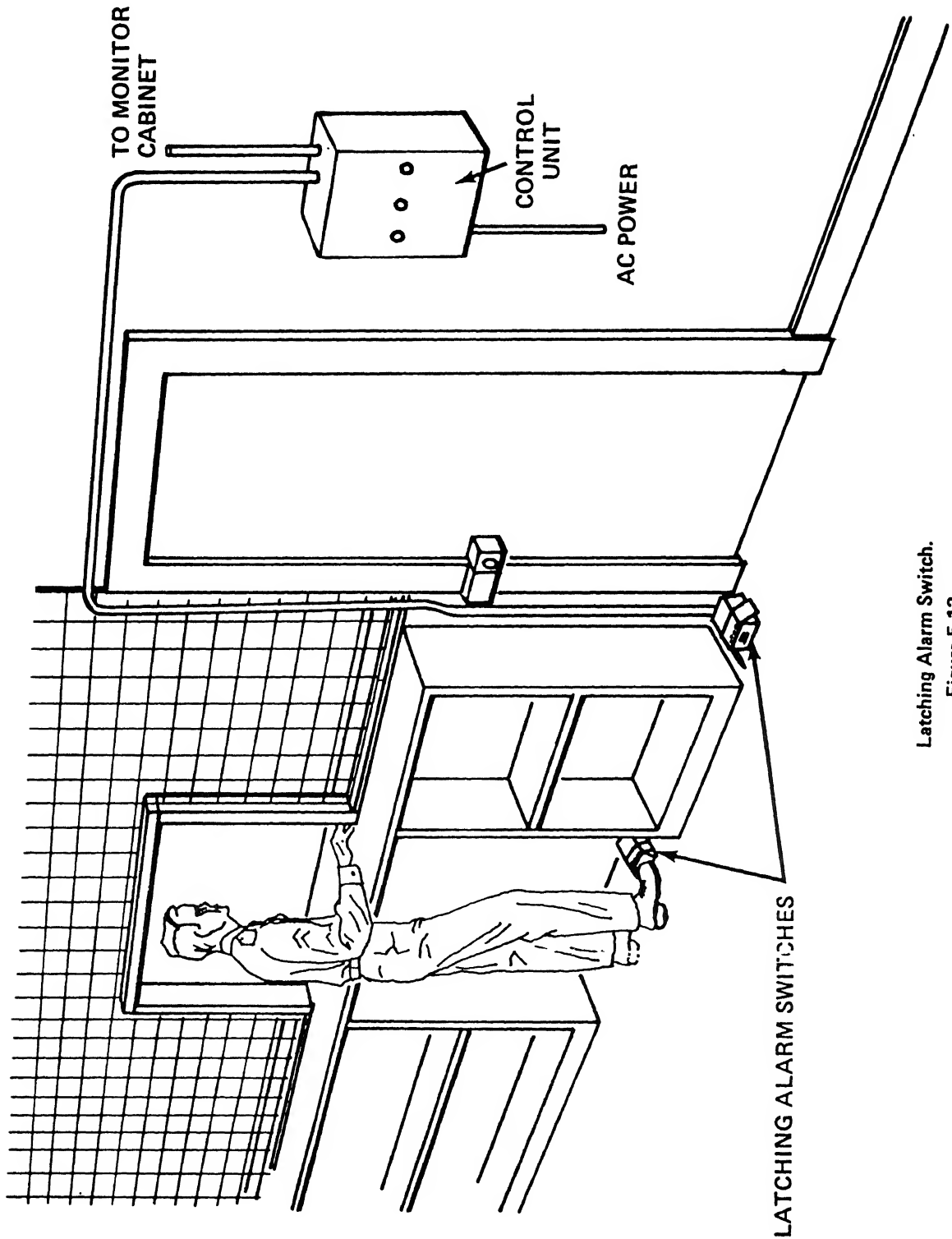
switch more susceptible to compromise. Loose fitting doors are a potential source of nuisance alarms when the balanced magnetic switch is used. Prior to installation of a balanced magnetic switch, every effort should be made to insure that the door is tight and well fitting. Openings in the door and in the other boundaries of the room can cause nuisance alarms when using the passive ultrasonic sensor.

- b. Exterior doors.* Exterior doors are those doors that lead into the secured area, i.e., are not wholly contained within the area. The balanced magnetic switch is used to detect the openings of these doors. The passive ultrasonic sensor, vibration sensor, or grid wire sensor is used to detect actual breakthrough of the door. The sensor chosen depends on the construction of the door. A door made of steel, or of wood covered with steel with the steel cladding inside the protected area, cannot be penetrated without producing ultrasonic energy. The passive ultrasonic sensor, therefore, gives adequate protection against penetration through such a door. A door that is made entirely of wood or wood substitute could be broken through without creating sufficient ultrasonic energy to activate the passive ultrasonic sensor. This type of door can be protected against breakthrough by installing the grid wire sensor on the inside surfaces of the door, or the inside of the door can be covered with sheet steel and the vibration sensor or the passive ultrasonic sensor can be installed to detect penetration attempts.

- c. Interior doors.* Interior doors are those doors that are wholly contained within the secured area, but are to be monitored for unauthorized opening. The degree of security required on an interior door can be reduced to that provided by a balanced magnetic switch. Breakthrough monitoring or detection is not necessary unless the contents of the area behind the interior door are particularly sensitive.

2. Walls, floors, and ceilings.

- a. Walls, floors, and ceiling,* the main body of the secure area, must be monitored for breakthrough at



Latching Alarm Switch.
Figure 5-12

16 SEP 1985

all points if a complete blanket of penetration detection is to be achieved. The detectors designed for this purpose are the grid wire sensor, the vibration sensor, and the passive ultrasonic sensor. The choice among these depends on the construction of the room.

b. Concrete and masonry structures can be monitored for penetration by installing the passive ultrasonic sensor. For the purpose of sensor component selection, there is little difference between reinforced concrete and masonry construction and nonreinforced concrete and masonry construction; however, it must be kept in mind that the time required to accomplish penetration of a reinforced concrete or reinforced masonry wall is longer than that required in the case of nonreinforced concrete or masonry wall.

c. A wooden structure is the easiest to penetrate and the most difficult to protect. Penetration detection can be afforded a wooden building by covering all surfaces (ceiling and floor included) with the grid wire sensor. An alternate approach is to install an expanded metal cage around the protected items, thus creating a secondary boundary and use a vibration sensor on the cage. This modification will greatly improve the physical security aspects of the building and give the reaction force a longer allowable response time. A third approach is the use of the passive ultrasonic sensor in conjunction with the ultrasonic motion sensor. It is imperative, however, that the room be sealed against outside sources of ultrasonic energy if the latter alternative is chosen.

d. A structure that is a combination of construction materials must be protected as the unique characteristics of the structure dictate. Where only a small section of wood or plaster is involved in an otherwise all concrete or masonry structure, this small section can be covered with sheet metal, thereby making the entire secure area suitable for use with the passive ultrasonic sensor. The deciding factor in the choice between the grid wire sensor and passive ultrasonic sensor is whether ultrasonic energy is generated when an attempt is made to penetrate the perimeter of the secure area. If ultrasonic energy is not generated, the procedures outlined in the foregoing subparagraph should be followed.

e. Openings in walls, doors, floors, and ceiling can create special problems in the use of the passive ultrasonic sensor as they may allow outside ultrasonic energy to enter the secure area and cause nuisance alarms. All openings (such as vents and exhausts) should be permanently sealed or covered with shut-

ters. Where a ventilation opening is required to be opened when the area is secured, the vent must be fitted with an ultrasonic baffle. The ringing of a normal telephone bell produces ultrasonic energy, thus all telephone bells in the secure area must be replaced with tone ringers available from the telephone company.

f. In an area where a high ambient ultrasonic noise level makes the passive ultrasonic sensor unusable, thought should be given to fabricating a secondary boundary within the secure area using an expanded metal cage to completely enclose the protected items and installing a vibration sensor. Because of the limited range of the vibration detectors (4 foot radius) and the limited number of detectors that can be connected to one signal processor (20), it may be necessary to use more than one vibration sensor to cover the entire cage.

g. In an area subject to very loud noises, the vibration sensor may be subject to nuisance alarms. This may also be true when transducers are mounted to barriers (metal roofs, metal outer walls, etc.) which are exposed to uncontrolled human or environmental activity (rain, hail, etc.). Under these circumstances a different sensor should be used. In any case, the vibration sensor should never be mounted on a nonmetallic barrier.

3. Windows.

a. These are another source of problems as they are particularly susceptible to penetration. Wherever possible, windows should be eliminated. If they are sealed over and their function replaced by artificial lights and ventilators, the window areas become part of the wall.

b. Where windows are necessary, consideration should be given to the use of interior metal shutters which can be closed and locked when the area is secured. Shutters give an added degree of penetration prevention and allow use of the passive ultrasonic sensor to monitor the window for intrusion. If the use of metal shutters is impractical, balanced magnetic switches can be used to detect unauthorized opening of the windows.

c. Where open work metal barriers (such as expanded metal grillwork or iron bars) cover the inside of a window, the passive ultrasonic sensor is recommended when the window is closed against outside ultrasonic energy. If the character of the room does not permit use of the passive ultrasonic sensor, the window may be secured with a vibration sensor or a capacitance proximity sensor. If the metal

16 SEP 1985

barrier is outside the window, an additional insulated-from-ground expanded metal grill should be installed on the inside of the window and coupled to the capacitance proximity sensor. If a noninsulated expanded metal grill covers the inside of the window, a vibration sensor should be installed on the grill. If the inside barrier consists of iron bars, an expanded metal grill can be welded to the bars and the vibration sensor mounted on the grill.

4. *Ventilation openings.*

a. These are openings in the ceiling, walls, and doors to allow the free passage of air. They are generally covered with steel mesh or louver barriers and are often large enough to admit an intruder. Some are required to ventilate only when the room is occupied and some are required regardless of the status of the room. All can admit ultrasonic energy generated outside the room.

b. For maximum protection against unwanted ultrasonic energy, consideration should be given to the elimination of ventilators. Sealed ventilators become part of the wall.

c. Where it is not feasible to seal the ventilators, consideration should be given to the use of locked metal shutters when the room is secured. This seals against the transmission of ultrasonic energy and allows the use of ultrasonic sensors in the room. Intrusion through the ventilator then can be detected with the passive ultrasonic sensor. Intrusion can also be detected with the vibration sensor mounted to the metal barrier or seal.

d. Where the ventilators are required to be open all the time, the aperture can be sealed against the passage of ultrasonic energy with a baffle over the inside; however, consideration must be given to the impeded air flow into or out of the room. Installation of the baffle allows the use of the passive ultrasonic sensor in the room. If ultrasonic baffles cannot be implemented, metal grills can be placed over the ventilator openings. This then allows the use of the vibration sensors mounted to the metal grill or the capacitance proximity sensor connected to the grill. The metal grill would be placed over the inside of the ventilator opening.

5. *Construction openings.* These are unsecured openings from incomplete construction. They should be completed and sealed over, in which case they become part of the wall. Where this is not feasible, a temporary expedient is to cover the opening with a grid wire sensor installed on fire-resistant plywood. Where the opening is required to stay open, a

capacitance proximity sensor can be used with an insulated metal grill over the inside of the opening.

6. *Air conditioners.* Air conditioners are generally set into a wall or window and are sometimes protected on the outside with a steel-bar barrier. To monitor for intrusion through the air conditioner aperture, the capacitance proximity sensor can be used on an insulated metal grill extending into the room in front of the unit.

7. *Ambient noise.* High ambient noise or occasional noise that is generated by the equipment in the room or by equipment outside the room and transmitted into the room through the walls, ceiling, floor, or openings will require care in the application of the passive ultrasonic sensor. Alarms may result from a series of short "banging," "cracking," or "popping" noises generated by steam pipes, water hammer, relief of structural stresses, or other causes.

0511. MOTION DETECTION

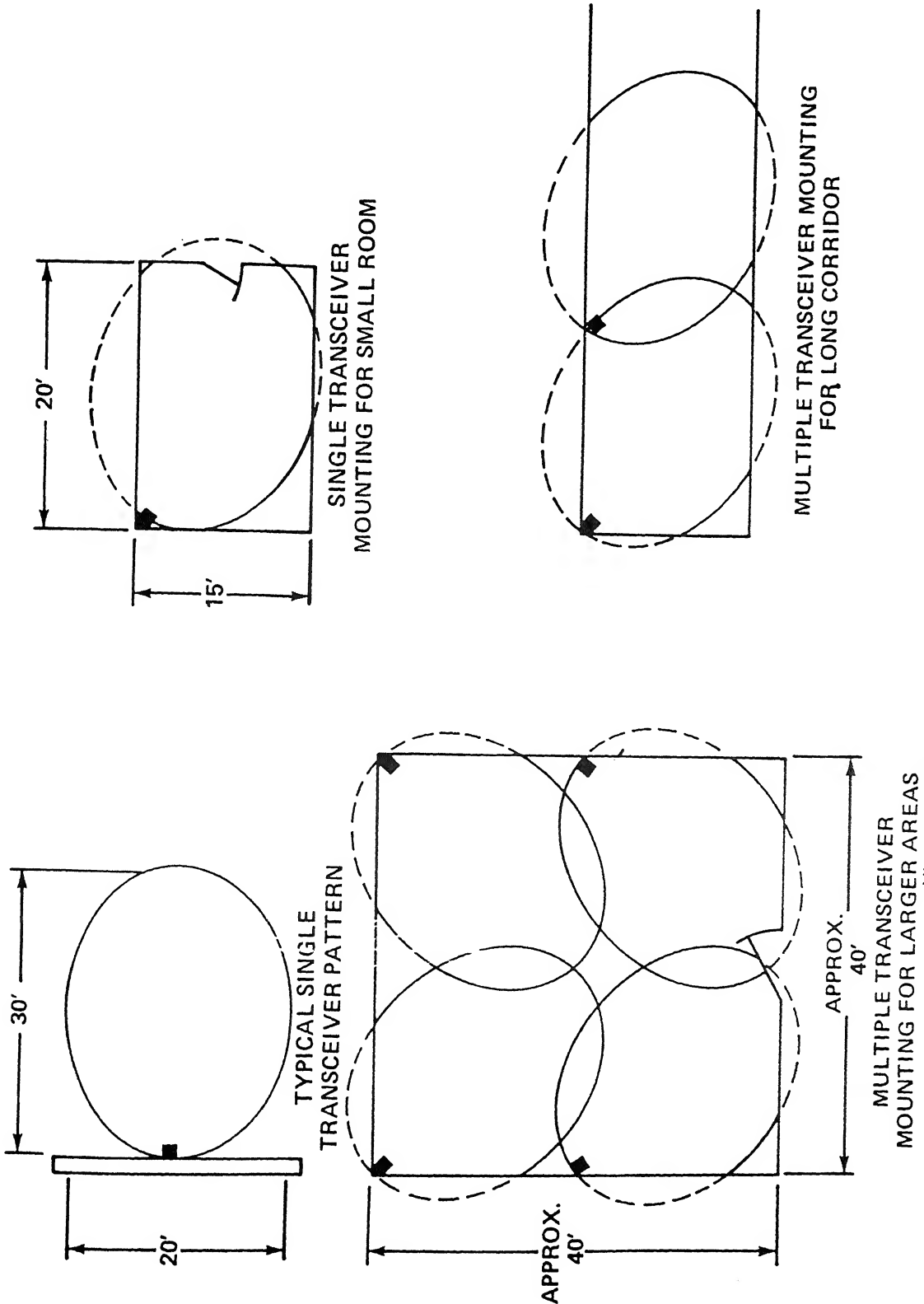
1. *General.* This type of detection is also called volumetric or space detection. This intermediate level of detection is very effective against the stay-behind intruder, the person who hides himself during hours of operation and carries out his theft after the room has been secured for the evening. This motion sensor also provides backup detection, with a corresponding decrease in allowable response time, to the penetration detectors.

2. *Ultrasonic motion sensor.*

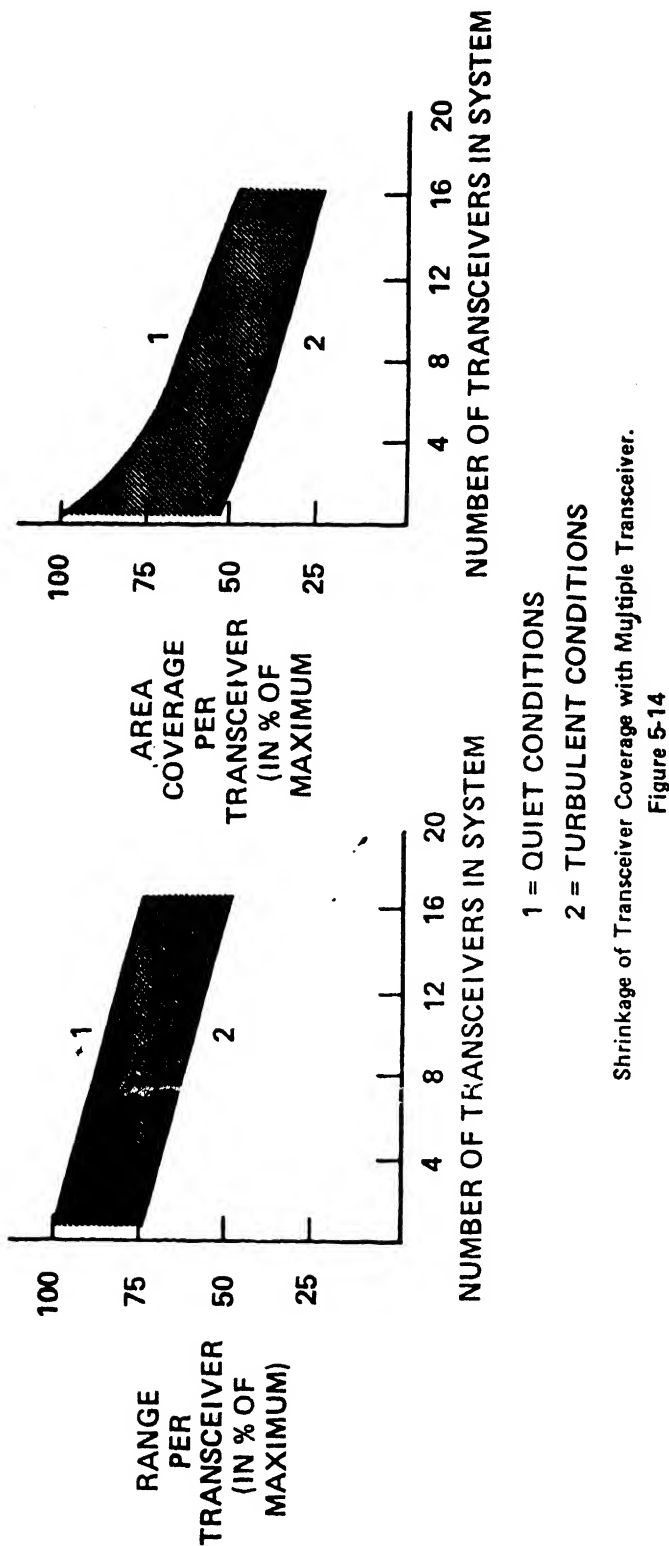
a. The ultrasonic motion sensor (UMS) is the only motion sensor currently incorporated into the J-SIDS. It should be used in any secure area that is adequately sealed against outside sources of ultrasonic energy.

b. Transceiver placement is important for optimum operation (see fig. 5-13). Each transceiver can cover an area up to 30 feet long and 20 feet wide when used in a "quiet location, i.e., relatively free of air turbulence. Actual coverage is a function of the reflection properties of a room to ultrasonic energy, the number of transceivers connected to the signal processor, and the general level of air turbulence and background ultrasonic noises (see fig. 5-14).

c. Each transceiver provides an egg-shaped volume of coverage with its maximum dimensions approximately as shown in figure 5-13. These areas will shrink as the number of transceivers connected to the signal processor and air turbulence increases.



Ultrasonic Motion Sensor Transceiver Emplacement.
Figure 5-13



16 SEP 1985

d. The most effective protection is given to areas within line of sight of a transceiver. Additional coverage is obtained through reflections, and depends on the particular geometry. Large objects in a room may produce insensitive areas on the side away from the transceiver. This is called "shading." Large rooms, which are compartmentalized by high furniture, equipment, racks, stacks of stored materials, et cetera, are best protected when they are regarded as several smaller rooms with each open (line of sight) area covered by a transceiver.

e. Transceivers should be placed so that the most likely intruder motions, such as through a doorway or along a corridor, are toward or away from the transceiver, rather than across the beam, in order to maximize the Doppler signal. If more than one transceiver is necessary to protect an area, it is mandatory that they all face in one direction so that they may reinforce one another.

For example: To protect a long hall, do not place transceivers at each end. Instead, place one at one end, and the second at the midway point, also facing the other end as shown in figure 5-13. An exception to this rule is when the corridor is more than 100 feet long—transceivers may then be placed at each end, facing each other. Transceivers should not be located higher than 8 feet above the floor.

f. Substantial air turbulence near the transceiver is a potential source of nuisance alarms and reduces the maximum target-detection range. Maximum coverage is obtained in still air. The transceivers should not be located adjacent to air ducts or radiators. Transceiver vibration can also cause reduced sensitivity; therefore, insure that wall vibrations cannot be felt at the transceiver mounting location when after-hours-operated machinery is on.

g. The number of transceivers required to cover a given area or number of rooms can be judged by the graphs in figure 5-14 which relate the typical maximum range for each transceiver to the number of transceivers in the system and levels of the background turbulence.

h. The ultrasonic motion sensor, when used in conjunction with the passive ultrasonic sensor, can also be used to provide penetration detection.

0512. POINT DETECTION

1. *General.* This innermost level of detection capability is the so-called "last line of defense" as it detects the attempted removal of protected items. It gives the least warning, in terms of time, to the reaction force.

2. The capacitance proximity sensor is designed for use on metal cabinets and will detect movement near a cabinet or contact with any part of the cabinet. As a metal cabinet is an all-purpose storage facility, the capacitance proximity sensor can be used in a variety of secure areas. One capacitance proximity sensor can protect up to 1,200 square feet of container surface area (total surface area to include all sides, top, and bottom).

3. A balanced magnetic switch alone mounted on the door of a metal cabinet does not provide adequate protection. The switch will become unbalanced and alarm if someone opens the cabinet door, but offers no protection against the intruder who seeks to cut through the cabinet with a hacksaw or torch.

4. Use of the capacitance proximity sensor is subject to the following constraints:

a. It cannot be applied to any items that cannot be electrically insulated from ground.

b. It should not be used close to high-power radio transmitters.

0513. DURESS SENSOR

The duress sensor is not included in the discussions concerning the three levels of detection capability; it is recommended for use wherever it is anticipated that duty personnel may be forced to yield protected items to unauthorized persons. The latching alarm switch is a duress sensor used to call for help. It consists of a switch that can be operated by hand or by foot. It should be located at a position most likely to be occupied by personnel in the secure area, but where it will not attract attention or be set off accidentally. Any number of switches may be used in series with one duress sensor input of the control unit.

0514. CONTROL UNIT

Each secure area must have a control unit to monitor the sensors in that secure area, supply DC power to the sensors, provide standby power, and process and relay the alarm and status signals to the monitor modules and audible alarm. The number of sensors that can be applied to a particular secure area is limited by the number of terminals in the control unit. The control unit has five intrusion sensor inputs plus a duress sensor input. This limitation does not affect the capability to use additional ultrasonic motion sensor, passive ultrasonic sensor, and vibration sensor transducers or multiple balanced magnetic

16 SEP 1985

switch or grid wire sensor sections on a single control unit intrusion sensor input circuit.

0515. MONITORING AND DISPLAY EQUIPMENT

1. *Monitor cabinet.* The monitor cabinet supplies power to the enclosed monitor modules, maintains standby power, and gives notice of its own signal and power status. Each monitor cabinet contains a source of standby DC power and one signal and power monitor module. Depending on the type of monitor cabinet ordered, from 1 to 25 monitor modules may be inserted into the cabinet. If the Data Transmission System, type I, is part of the system, the data receiver is also housed in the monitor cabinet. It is advisable to order a monitor cabinet that will allow for future expansion rather than just meet present needs.

2. *Status and alarm monitor modules.* Each control unit will transmit its alarm and status signals to a separate monitor module located in the monitor cabinet. Thus for every control unit used, a corresponding monitor module must be used. Two types of monitor modules are available. The first is the status monitor module. This module notifies duty personnel of the system's (system here meaning a control unit and associated sensors) mode of operation, AC power status, and alarm condition. The second type of module, the alarm monitor module, only gives notice of an alarm condition. The status monitor module is used whenever complete system status is to be monitored.

0516. LINE SECURITY

All hardwire (unsupervised) connections between the sensors in a particular secure area and their corresponding control unit must be encased in rigid steel conduit to make line tampering more difficult. Line security between the control unit and monitor module can be achieved in two ways. First, the hardwire (unsupervised) connection can be encased in conduit from end to end and then buried underground or encased in concrete. This becomes difficult and costly when the monitoring station is located at a great distance from the particular secure area. Second, a data transmission system could be used to provide transmission security and line supervision. It is recommended that a data transmission system be installed whenever the lines between the control unit and the monitor module cannot be provided with complete end-to-end physical protection or when line supervision is required.

0517. AUDIBLE ALARM

The audible alarm is located outside the protected room or building. It can serve as a deterrent to scare a would-be intruder away and to alert guard forces and other personnel in the area. The use of this device alone, without a remotely located monitoring capability, is not recommended. For reasons covered previously, the audible alarm is not activated by the latching alarm switch (duress sensor).

Part 5. System Selection Procedure

0518. GENERAL

The purpose of this section is to provide a procedure for the selection of the appropriate intrusion detection system for a particular facility. Important to this selection process is a complete understanding of the information regarding the operating characteristics of the available devices, and the use of these devices to provide security for various physical situations. The selection process is implemented by first conducting a detailed survey of the facility and then selecting the appropriate devices using the Component Selection Tables.

0519. PHYSICAL SURVEY

In order to select the appropriate type and number of J-SIIDS devices, it is necessary to conduct a detailed

survey of the facility. The location of the rooms and the size, shape, and materials of construction of the walls, ceilings, floor, doors, windows, and other openings should be noted. The distribution, size, and shape of safes, cabinets, and other objects in the rooms should also be noted. Once this information has been gathered, the appropriate types and numbers of devices can be selected.

0520. SELECTION PROCEDURE

1. *General.* Figure 5-15 is provided as an aid in selecting the appropriate system component. The tables list the various features of the room to be identified during the preselection survey and the recommended sensor to be used to provide detection of intrusion.

16 SEP 1985

2. *Penetration sensors.* Detection of penetration through the perimeter of the facility provides the reaction force with the maximum "time to respond." The facility should be provided with this level of detection and care should be taken that the entire perimeter of the facility is protected against penetration. Figure 5-15 is provided to aid in selection of sensors that will provide this detection.

3. *Motion sensors.* A minimum of two levels of detection capability should be provided. Only one motion sensor, the ultrasonic motion sensor, is available at the present time. Selection of this sensor is based on the requirements and constraints discussed in part 4.

4. *Point sensors.* Point sensors can be selected to provide the second level of detection by detecting attempted removal of the protected item. The capacitance proximity sensors depicted in figure 5-15 will provide this capability.

5. *Duress sensor.* Only one duress sensor, a latching alarm switch, is available at the present time. Selection of this sensor is based on the requirements and constraints discussed in paragraph 0513. Note that any number of duress sensors can be connected to the single duress sensor input of the control unit.

6. *Control unit.* One control unit is required for each area to be secured and uniquely identified by its own status or alarm module.

7. *Monitor cabinet.* Three sizes of monitor cabinets are available: a single-zone cabinet, a five-zone cabinet, and a 25-zone cabinet. Judgment should be exercised in selection of a monitor cabinet to allow for system expansion; e.g., it may be more cost-effective to select a five-zone cabinet rather than two or three single-zone cabinets. Note that the status and

alarm monitor modules which plug into the monitor cabinet are not an integral part of the monitor cabinet and must be ordered separately. One monitor module is required for each control unit that is to be monitored.

8. *Data transmission system.* A data transmission system is recommended to interconnect the control unit and monitor cabinet whenever:

- a. Telephone systems are to be used.
- b. The control unit and monitor cabinet are not within the same building.
- c. Line supervision is required.

A data transmission system is required for each control unit and monitor module combination. Multiple (up to five) data transmission systems can be multiplexed onto a single transmission line pair.

9. *Audible alarm.* The audible alarm is not recommended for use in remote areas except where its use is to be limited to a deterrent. The use of the audible alarm as the only system notification device is not recommended. When used in conjunction with the monitor modules, it is useful to alert local guard forces and personnel in the immediate area to an alarm condition and can often be used as a deterrent by alerting would-be intruders to the fact that their attempted intrusion has been detected.

10. *Other criteria.* After the facility has been thoroughly surveyed and evaluated and selection of sensors has been completed, the following questions should be addressed:

- a. Do the sensors that have been selected give complete and dual levels of protection? If not, are additional sensors required or are construction modifications required?
- b. Have possible sources of nuisance alarms been considered in the selection of sensors?

Part 6. Procurement

0521. GENERAL

The procedures to be followed in the procurement of

J-SIIDS components will be promulgated when they become available.

16 SEP 1985

Intrusion through: (method)	Construction material	Recommended sensor	Area coverage per sensor	Notes
Exterior door* (breakthrough)	Metal or metal clad on inside	Passive Ultrasonic	15 ft. by 20 ft. per transducer	Room must be sealed from outside sounds
Exterior door* (breakthrough)	Wood or wood substitute	Vibration	4 ft. radius per transducer	Mounted at approximate center of door
Exterior door* (pening)	N/A	Grid wire kit	160 sq. ft. per kit	
Exterior door* (pening)	N/A	Balanced magnetic switch	N/A	
Exterior door* (pening)	N/A	Balanced magnetic switch	N/A	
Exterior door* (breakthrough)	Metal or metal plate covered on same side as sensor	Passive ultrasonic	15 ft. by 20 ft. per transducer	Room sealed from outside sounds
Exterior door, Ceiling	Wood	Vibration	4 ft. radius per transducer	Mounted at approximate center of door
Exterior door, Ceiling	Plaster	Grid wire kit	160 sq. ft. per kit	
Exterior door, Ceiling		Passive Ultrasonic and ultrasonic motion sensors	Limited to individual sensor coverage	Must always be used in combination
Exterior door, Ceiling	Metal	Passive ultrasonic	15 ft. by 20 ft. per transducer	Max. 20 transducers per processor—room sealed from outside sounds
Exterior door, Ceiling	Masonry	Vibration	4 ft. radius per transducer	
Exterior door, Ceiling	Metal wire mesh bars	Grid wire kit bars	160 sq. ft. per kit	Additional fire-resistant wooden wall inside required
Exterior door, Ceiling	Metal wire mesh bars	Passive ultrasonic	15 ft. by 20 ft. per transducer	Additional fire-resistant wooden wall outside required
Exterior door, Ceiling	Glass and open work metal barrier (bars/mesh)	Vibration	4 ft. radius per transducer	
Exterior door, Ceiling		Passive ultrasonic	15 ft. by 20 ft. per transducer	Room sealed from outside sounds

*Exterior door is any door opening into the secure area whether indoors or out; interior door is any door wholly within the secure area.

16 SEP 1985

Intrusion through: (method)	Construction material	Recommended sensor	Area coverage per sensor	Notes
Exterior door* (Breakthrough)	Metal or metal clad on inside	Passive Ultrasonic	15 ft. by 20 ft. per transducer	Room must be sealed from outside sounds
Exterior door* (Breakthrough)	Wood or wood substitute	Vibration	4 ft. radius per transducer	Mounted at approximate center of door
Exterior door* (Breakthrough)	N/A	Grid wire kit	160 sq. ft. per kit	
Exterior door* (Breakthrough)	N/A	Balanced magnetic switch	N/A	
Exterior door* (Breakthrough)	N/A	Balanced magnetic switch	N/A	
Exterior door* (Breakthrough)	Metal or metal plate covered on same side as sensor	Passive ultrasonic	15 ft. by 20 ft. per transducer	Room sealed from outside sounds
Exterior door* (Breakthrough)	Wood	Vibration	4 ft. radius per transducer	Mounted at approximate center of door
Exterior door* (Breakthrough)	Plaster	Grid wire kit	160 sq. ft. per kit	
Exterior door* (Breakthrough)		Passive Ultrasonic and ultrasonic motion sensors	Limited to individual sensor coverage	Must always be used in combination
Exterior door* (Breakthrough)	Metal	Passive ultrasonic	15 ft. by 20 ft. per transducer	Max. 20 transducers per processor—room sealed from outside sounds
Exterior door* (Breakthrough)	Masonry	Vibration	4 ft. radius per transducer	Additional fire-resistant wooden wall inside required
Exterior door* (Breakthrough)	Metal wire mesh bars	Grid wire kit bars	160 sq. ft. per kit	Additional fire-resistant wooden wall outside required
Exterior door* (Breakthrough)	Metal wire mesh bars	Passive ultrasonic	15 ft. by 20 ft. per transducer	
Exterior door* (Breakthrough)	Glass and open work metal barrier (bars/mesh)	Vibration	4 ft. radius per transducer	
Exterior door* (Breakthrough)		Passive ultrasonic	15 ft. by 20 ft. per transducer	Room sealed from outside sounds

*Exterior door is any door opening into the secure area whether indoors or out; interior door is any door wholly within the secure area.

APPENDIX XIII

MINIMUM TRAINING STANDARDS FOR SECURITY FORCE PERSONNEL

PHASE ONE

1-1. ADMINISTRATIVE SUBJECTS

- a. Overview - Role of Security Force Personnel
- b. Security Department Organization - Duties and Responsibilities
- c. Standards of Conduct and Appearance
Professional Law Enforcement Ethics
- d. Forms and Reports
Report Writing
- e. ID's, Decals and Passes - Personnel and Vehicles
- f. Area Familiarization

1-2. LEGAL SUBJECTS

- a. Jurisdiction and Authority
Posse Comitatus
- b. Rules of Evidence
- c. Search and Seizure
- d. Substantive Criminal Law
- e. Self-Incrimination, Admissions and Confessions
- f. Apprehension and Arrest
Stop and Frisk
- g. Detention and Confinement
- h. Federal Magistrate System (Act)
- i. Status of Forces Agreement

OPNAVINST 5530.14A

16 SEP 1985

1-3. TRAFFIC LAWS AND ENFORCEMENT

- a. Military Traffic Law and Enforcement
- b. Mishap Investigation and Reporting
Hit and Run
- c. Driving Under the Influence
Enforcement
Implied Consent
- d. Traffic Control and Direction
- e. Parking Enforcement and Impounding Vehicles

1-4. PATROL PROCEDURES

- a. Radio Communications
"10"-Code
- b. Routine and Specialized Building and Repository Checks
Escorts
- c. Vehicle Stops
Search of Vehicles (Random and probable cause (warrants))
- d. Crimes in Progress
- e. Physical Security Safeguards

1-5. UNUSUAL INCIDENTS

- a. Terrorism
- b. Bomb Threats, Wrongful Destruction and Sabotage

1-6. PROFESSIONAL SKILLS

- a. Driver Training (DOT EVOC) (optional)
- b. Weapons Proficiency Training
- c. Use of Force
- d. Defensive Tactics
- e. Physical Training

MINIMUM TRAINING STANDARDS FOR SECURITY FORCE PERSONNEL

PHASE TWO

2-1. ADMINISTRATIVE SUBJECTS

- a. Recording, Handling and Disposition of Property
Missing, Lost, Stolen, or Recovered (MLSR) Government
Property Reporting
- b. Information Security
- c. Absentees and Deserters
- d. Public Relations

2-2. LEGAL SUBJECTS

- a. Juvenile offenses
- b. Judicial Proceedings
Testimony and Demeanor

2-3. TRAFFIC LAWS AND ENFORCEMENT

- a. Selective Enforcement
- b. Crime Prevention

2-4. CRIMINAL INVESTIGATIONS

- a. Jurisdiction and Responsibilities
Felonies
- b. Crime Scene - Identification, Preservation, and Collection
of Evidence. Notes - Sketches - Photography
- c. Identification of Victims, Witnesses, and Suspects
Showups
Line-ups
- d. Interviews and Interrogations
Notetaking
Statements
- e. Managing Informants
- f. Crimes Against Persons
- g. Crimes Against Property

16 SEP 1985

h. Drugs of Abuse - Identification, Prevention and Control

i. Vice Investigations
Armed Forces Disciplinary Control Boards

2-5. UNUSUAL INCIDENTS

a. Disaster and Emergency Planning

b. Civil Disturbances
Crowd/Mob Psychology and Control

c. Hostage Situations and Barricaded Suspect(s)
Scene Security and Notifications

d. Animal Complaints

e. Human Services - Missing Persons, Found Children, and Senile Persons

f. Family Intervention
Spouse Abuse
Child Abuse
Domestic Conflict

g. Recognizing and Handling Abnormal Behavior
Alcoholism
Drug Abuse
Mental Disorders

2-6. PROFESSIONAL SKILLS

a. Chemical Agents
b. Breath Testing and Radar Certification
c. Fingerprints - Rolled and Latent
d. Emergency Medicine/Trauma Management
e. Physical Training

16 SEP 1985

APPENDIX XIII - TAB AFIREARMS PROFICIENCY1. COURSE OF INSTRUCTION

a. Purpose. All personnel assigned to a law enforcement/physical security function and who are designated and authorized to carry a weapon shall receive a minimum of 16-hours of firearms instruction as prescribed herein:

<u>TOPICS</u>	<u>HOURS</u>
Policy - Regulations-----	2
Use of Force Safety/Nomenclature-----	1
Liability-----	1
Judgement Pistol Shooting "Shoot-Don't Shoot"	
Officer Safety/Survival-----	4
Pistol Familiarization and Qualification (Combat Pistol Course)	
Shotgun Familiarization-----	8
	TOTAL = 16

b. Range Officers. At each command, a qualified member shall be appointed to act as range officer. He/she will be a certified firearms instructor. The range officer shall give all commands while on the firing range and will be responsible for the enforcement of proper range safety practices by all personnel on the range.

2. COMBAT PISTOL COURSE

a. Range Specifications. The revised Combat Pistol Course (CPC) is designed to be fired on a 25-yard range, utilizing standard silhouette targets and turning type targets, if available. The firing points are located at the three yard line, seven yard line, 15 yard line and 25 yard line.

b. Range Safety Rules

(1) Before firing, inspect the weapon for worn parts, plugged or damaged barrel, etc.

16 SEP 1985

(2) Do not remove weapon from holster until at the firing point facing the target, or at a place designated for dry firing, and only when instructed to do so. If it is necessary to carry a weapon in hand, swing the cylinder open.

(3) Do not load or cock a weapon until instructed to do so.

(4) Listen for and obey all range commands instantly.

(5) When unloading a weapon, keep it pointed down-range.

(6) Never talk to a shooter on the firing line unless you are the coach or the range officer.

(7) If any unsafe condition is observed, immediately call "cease fire" and notify the range officer.

(8) When drawing a weapon, keep the trigger finger off the trigger until the weapon is pointed down-range.

(9) In case of a misfire or a jam, keep the gun pointed down-range and notify the range officer by raising the non-shooting arm.

(10) Cartridges being carried in a shooter's firearm and cartridge pouch should be fired during each firearm training session and replaced with fresh ammunition.

(11) Never proceed to the targets without the command of the range officer.

(12) Ear protectors ("doughnuts" or plugs) are required at all times when firearms are being discharged during training and familiarization sessions.

(13) Range safety eyeglasses or other shatterproof eyeglasses are required when firing.

c. General Firing Rules

(1) Every firearm should be considered loaded until such time as it has been examined and proven otherwise. Never trust one's own, or anyone else's memory as to the status of a firearm.

(2) Never point a weapon at anyone or anything unless one intends and is justified to shoot, nor in any direction where a discharge might do harm.

(3) Never insert the finger inside the trigger guard unless prepared to discharge the weapon.

(4) Never cock the firearm unless prepared to discharge.

(5) Before loading ammunition into the firearm, check for dirt, excess oil, grease, malformations, or other defects. Check the bore to be sure it is free of foreign matter or obstructions.

(6) Never leave firearms unguarded or unsecured for even a brief period of time.

(7) Never discharge a firearm when running. Always stop first, support the weapon and fire only when certain of the target and the path of the projectile.

(8) Never load the firearm with dented cartridges, cartridges with loose bullets, cartridges eaten away by corrosion, or in any other way damaged.

d. Range Procedures

(1) Weapons will not be loaded until the command is given by the range officer at each phase of the course.

(2) At the end of each phase of the course, all weapons will be unloaded and holstered before any commands are given to leave the range.

e. Suggested Range Commands

(1) The commands to commence and cease fire will be given with a police whistle or bullhorn as follows:

(a) Commence fire.....One short blast/"Commence Fire."

(b) Cease fire.....One long blast/"Cease fire."

(NOTE: If turning targets are used, shooters will fire when the target faces and cease firing when the target edges.)

(2) The commands to be given on the range are as follows:

(a) "With X rounds, load and holster your weapon."

(NOTE: X = The number of rounds specified for each of the various sequences of fire.)

(b) "With X rounds, load your ammunition pouch."

(c) "Is the line ready?" "The line is ready."

(d) "Ready on the left, ready on the right?" (If everyone is ready) "All ready on the firing line."

(e) (After a three-second interval) Commence firing command.

(f) (After Y seconds) Cease firing command.

(NOTE: Y = The number of seconds specified for each of the various sequence of fire.)

(g) "Any alibis?" (If there are any "alibis" (unfired rounds), allow the shooter(s) to fire them to the left of the target and they are not scored.

(NOTE: Shooters shall be penalized five points each for each shot fired after the initial cease fire command and before permission to fire the alibis is given.)

(h) "Clear your weapon."

(i) "Holster your weapon."

(j) (After all weapons are cleared and holstered) "Score the target to the right. Last position score number one target."

f. Course of Fire - .38 6-shot Revolver

(1) Three Yard Line. Twelve rounds, double action, quick point position. The shooter stands with the weapon empty and holstered with 48 rounds available. On the command of the range officer, the shooter will load six rounds and holster the weapon. The shooter will then load six rounds in the ammunition pouch. On the command of the range officer, the shooter will draw the weapon and assume a quick point position, fire two rounds, and cover the target until instructed to holster by the range officer. On the command of the range officer, the shooter will draw and fire two rounds from the quick point position and then cover the target until instructed to holster by the range officer. Time limit four seconds for drawing and firing each two round sequence. On the command of the range officer, the shooter will draw and fire two rounds from the quick point position, immediately combat unload the expended rounds, load two rounds from the ammunition pouch, fire those rounds from the quick point position, and then cover the target. When instructed by the range officer, the shooter will combat unload

and reload two additional rounds from the ammunition pouch, and holster the weapon. On the command of the range officer, the shooter will draw and fire two rounds from the quick point position, immediately combat unload the expended rounds, and reload two rounds from the ammunition pouch, and fire those rounds from the quick point position and then cover the target until instructed by the range officer to unload and holster the weapon. Time limit is fifteen seconds for each four round sequence.

(2) Seven Yard Line. Twelve rounds, double action, quick point position, same as above.

(3) Fifteen Yard Line. Twelve rounds, double action, point shoulder position, same as above.

(4) Twenty-Five Yard Line. Twelve rounds, double action, barricade position. The shooter stands behind the barricade with the weapon empty and holstered. On the command of the range officer, the shooter loads six rounds in the weapon, holsters and then loads six rounds in the ammunition pouch. On the command of the range officer, the shooter will draw the weapon and fire six rounds from the right side barricade position. The shooter will then immediately combat unload the expended rounds, reload with six rounds from the ammunition pouch and fire six rounds from the left side barricade position. The shooter will cover the target until instructed to unload and holster by the range officer. Time limit one minute.

g. Course of Fire - .45 Semi-Automatic and 9mm Semi-Automatic Pistols

(1) Three Yard Line. Ten rounds, quick point position. The shooter stands with the weapon empty and holstered with 40 rounds and two magazines available. On the command of the range officer, the shooter will insert a five round magazine in the weapon, holster, and have a five round magazine available. On the command of the range officer, the shooter will draw the weapon and assume a quick point position, fire two rounds and continue to cover the target until instructed to holster by the range officer. On the command of the range officer, the shooter will draw and fire two rounds from the quick point position and then cover the target until instructed to holster by the range officer. Time limit is four seconds for drawing and firing each two round sequence. On the command of the range officer, the shooter will draw the weapon, fire one round from the quick point position, immediately drop the empty magazine, insert the spare magazine, fire one round from the quick point position and then cover the target. Time limit is ten seconds for this phase. On the commands of the

16 SEP 1985

range officer, the shooter will then repeat the same two round phases as set forth above.

(2) Seven Yard Line. Ten rounds, quick point position, same as above.

(3) Fifteen Yard Line. Ten rounds, point shoulder position, same as above.

(4) Twenty-five Yard Line. Ten rounds, barricade position. The shooter stands behind the barricade with the weapon empty and holstered. On the command of the range officer, the shooter inserts a five round magazine in the weapon, holsters, and has a five round magazine available. On the command of the range officer, the shooter will draw the weapon and fire five rounds from the right side barricade position, strong hand. The shooter will then immediately drop the empty magazine, insert the spare magazine and fire five rounds from the left side barricade position, strong hand. The shooter will then cover the target until instructed to drop the empty magazine and holster by the range officer. Time limit is one minute.

h. Scoring the Combat Pistol Course

(1) Scoring should be done using the "K" values on the target.

(2) Scoring with the 5-shot revolver:

Possible score-----200

Minimum qualifying score-----130

Marksman-----131-160

Sharpshooter-----161-180

Expert-----181-194

Distinguished expert-----195-200

(3) Scoring with the 6-shot revolver:

Possible score-----240

Minimum qualifying score ----180

Marksman-----181-205

Sharpshooter-----206-222

Expert-----223-232

Distinguished Expert-----233-240

(4) Scoring with the .45 and 9mm Semi-Automatic
Pistols:

Possible score-----200

Minimum qualifying score-----130

Marksman-----131-160

Sharpshooter-----161-180

Expert-----181-194

Distinguished Expert-----195-200

3. FAMILIARIZATION FIRE COURSE

a. Objectives. Ideally, all security force personnel authorized to carry firearms, should be required to qualify quarterly utilizing the Combat Pistol Course (CPC). However, time and ammunition restraints will in most instances make this goal untenable and necessitate alternatives. One is the Familiarization Fire Course which is designed for 12 rounds of ammunition with six additional rounds optional, depending on availability. Firearm qualification utilizing the CPC is required annually and Familiarization Fire Course during the other three quarters of the year for which a qualifying score must also be attained.

b. Special Regulations for Familiarization Fire Course.
All shooting for this course is done double action.

c. Course of Fire - .38 caliber, 5 or 6 shot Revolver

(1) Three Yard Line. Four rounds, double action, quick point position. The shooter stands with the weapon empty and holstered with twelve rounds available. On the command of the range officer, the shooter will load six rounds (four if a five-shot revolver) and holster the weapon. On the command of the range officer, the shooter will draw the weapon and assume quick point position, fire two rounds, and cover the target until instructed to holster by the range officer. On the command of the range officer, the shooter will draw and fire two rounds from the quick point position and then cover the target until instructed to holster by the range officer. Time limit is four seconds for drawing and firing each two round sequence.

(2) Seven Yard Line. Four rounds, double action, quick point position. If a 5-shot revolver, the shooter stands with the weapon empty and on the command of the range officer loads two rounds. On the second command of the range officer, the shooter will draw the weapon, fire two rounds from the quick position, immediately combat unload the expended rounds, load two rounds from the ammunition pouch, fire those rounds from the quick point position, and then cover the target until instructed to holster by the range officer. Time limit is fifteen seconds for this four round sequence.

(3) Fifteen Yard Line. Four rounds, double action, quick point position. The shooter stands with the weapon empty. On the command of the range officer, the shooter will load two rounds and holster the weapon. On the command of the range officer, the shooter will draw and fire two rounds from the quick point position, immediately combat unload the expended rounds, load two rounds from the ammunition pouch, fire those rounds again from the quick point position, and then cover the target until instructed to holster by the range officer. Time limit is fifteen seconds for this four round sequence.

(4) Twenty-five Yard Line (Optional and not utilized to compute the score, if fired). Six rounds, double action, barricade position. The shooter stands behind the barricade with the weapon empty and holstered. On the command of the range officer, the shooter loads three rounds in the weapon, holsters, and then loads three rounds in the ammunition pouch. On the command of the range officer, the shooter will draw the weapon and fire three rounds from the left side barricade position. The shooter will then immediately combat unload the expended rounds, load three rounds from the ammunition pouch, fire the three rounds from the right barricaded position, and cover the target until instructed to holster by the range officer. Time limit is forty-five seconds for the six round sequence.

d. Course of Fire - .45 caliber and 9mm Semi-Automatic. Familiarization fire for the .45 caliber semi-automatics shall be basically the same course as set forth above for the .38 caliber 5 or 6-shot revolver. The only difference shall be that the shooter will load a magazine into the pistol with the specified number of rounds for each sequence and have a magazine with the specified number of rounds available, when required, for the combat unload/load sequences.

e. Scoring Familiarization Fire.

(1) Scoring should be done utilizing the "K" values on the target.

(2) Possible score -----60

Minimum qualifying score-42

4. Nightfire Exercise

a. Objectives. Most Navy security force firearms training takes place on an outdoor range, during daylight hours, and under optimal weather conditions. Many security force shootings occur under less than optimal weather conditions resulting in diminished light or darkness. In order to familiarize security force personnel with the inherent handicaps of night fire and the necessary compensations, the Nightfire Exercise set forth below should be fired annually in lieu of one of the three quarterly Familiarization Fires. This course of fire is designed to be fired on a regulation, outdoor range utilizing vehicle headlights for those sequences where diminished light is required. This same course of fire may be utilized for those specially equipped nightfire ranges without modification.

b. Special Regulations and Instructions for the Nightfire Exercise

(1) When firing, weapons should be held below the line of sight, i.e., not the point shoulder position. The rationale for this is that the muzzle flash can severely impair the shooter's night vision.

(2) Shooters must be able to combat unload and load by feel due to the darkness or impaired light of the course of fire.

(3) All firing for this course is done double action.

c. Course of Fire - .38 caliber 5 or 6-shot Revolver

(1) Three Yard Line. Four rounds, double action, target illumination by a vehicle's headlights parked behind the seven yard line of fire. The shooter stands with the weapon empty and holstered with twelve rounds available. On the command of the range officer, the shooter will load four rounds and holster the weapon. On the command of the range officer, the shooter will draw the weapon, fire two rounds, and cover the target until instructed to holster by the range officer. On the command of the range officer, the shooter will draw and fire two rounds, then cover the target until instructed to holster by the range officer. Time limit is four seconds for drawing and firing each two round sequence. The headlights are then extinguished and on the command of the range officer, the shooter will combat unload the expended rounds, load four rounds, and holster the weapon.

On the command of the range officer, the shooter will move to a position on the seven yard line.

(2) Seven Yard Line - Phase 1. Four rounds, two rounds per four seconds, double action, total darkness, same sequence as above.

(3) Seven Yard Line - Phase 2. Four rounds, two rounds per four seconds, double action, same sequence as above without loading after firing the second two rounds and utilizing a flashlight versus total darkness. The shooter holds the flashlight in the weak, non-shooting hand. When the weapon is drawn on the command of the range officer, the shooter will turn the flashlight on and hold it on the target up and away from the body. After firing each two rounds of the sequence, the shooter will turn the flashlight off.

d. Course of Fire - .45 caliber and 9mm Semi-Automatic. The nightfire exercise for the .45 pistol shall be basically the same course as set forth above for the .38 caliber 5 or 6-shot revolver. The only difference shall be that the shooter will load a magazine into the pistol with the specified number of rounds for each sequence and have a magazine with the specified number of rounds available, when required, for the combat unload/load sequences.

e. Scoring the Nightfire Exercise

(1) Scoring the nightfire exercise is done by counting the number of hits within the silhouette target verses the "K" values. Shooters will not normally be disqualified from carrying weapons for a failure to qualify on this course of fire. The intent of this course of fire is more to familiarize the shooter with firing under conditions of impaired light or darkness. A failure to qualify would indicate a need for additional familiarization.

(2) Possible score ----- 12

Minimum qualifying score --- 8

5. Transition Course

a. Objective. Although security force personnel may find themselves in many situations in which they may have to use their sidearms, there are only six alternatives as to how they will actually fire them. Those are 1) strong hand, 2) weak hand, 3) single action, 4) double action, 5) one hand, and 6) two hands. Those six ways of firing constitute the basic skills of security force shooting, mastery of which will result in

enhanced Combat Pistol and Familiarization Course scores. The Transition Course is not meant to be a sidearms qualification course, but is designed as a basic skills training and development course of fire.

b. Course of Fire - .38 caliber 5 or 6-shot Revolver

(1) Fifteen Yard Line. Four stages, twelve rounds per stage (ten if a five shot), quick point position without support. The shooter stands with the weapon empty and holstered with forty-eight rounds available (forty if a five shot). On the command of the range officer at the beginning of each stage, the shooter will load six rounds (five if a five shot) and holster the weapon. Loading from a cartridge carrier or pocket is optional. On the command of the range officer for each stage, the shooter will draw and fire six rounds (five if a five shot), combat unload the expended rounds, load with six rounds (five if a five shot), and fire. Time limit is sixty seconds per stage (fifty if a five shot). The four stages of fire are as follows:

(a) Stage One - Ten or twelve rounds, strong hand, single action.

(b) Stage Two - Ten or twelve rounds, strong hand, double action.

(c) Stage Three - Ten or twelve rounds, weak hand, single action.

(d) Stage Four - Ten or twelve rounds, weak hand, double action.

c. Course of Fire - .45 caliber and 9mm Semi-Automatic

(1) Fifteen Yard Line. The Transition Course for pistols shall be exactly the same as for .38 caliber 5-shot revolvers with each stage consisting of ten rounds for a total of forty rounds. At the command of the range officer at the beginning of each stage, the shooter will insert a five round magazine in the weapon, holster, and have five round magazine available. On the command of the range officer for each stage, the shooter will draw and fire five rounds, drop the empty magazine, insert the spare magazine, and fire.

16 SEP 1985

d. Scoring the Transition Course

(1) Scoring the Transition Course shall be done by counting the number of hits within the silhouette target to establish a satisfactory or unsatisfactory rating. An unsatisfactory rating merely indicates a need for additional training and development of basic skills.

(2) Rating with the 6-shot revolver:

Possible Score	-----	48
Satisfactory	-----	32+
Unsatisfactory	-----	31-

(3) Rating with the 5-shot revolver or semi-automatic pistol:

Possible Score	-----	40
Satisfactory	-----	27+
Unsatisfactory	-----	26-

6. Shotguns

a. Safety Rules

(1) When loading a shotgun, keep the weapon vertical to the ground, muzzle up.

(2) The safe condition of a shotgun is unloaded, action open, and safety on. When carrying the weapon on the range, when benching it, or receiving it from or handing it to another person, make certain it is in this condition.

(3) Never put a finger through the trigger guard to set or release safety.

(4) Never snap the trigger to release the action. Use the action release.

(5) After unloading a shotgun, visually examine the chamber and the magazine to make certain the weapon is unloaded.

(6) When transporting a shotgun in a vehicle, it is recommended that it be unloaded. When it becomes necessary to transport it in a loaded condition, a shell should not be chambered, but rather have four rounds in the magazine and the safety on.

(7) A shotgun will be brought to a firing position (i.e., leveled at the suspect or target) and the safety taken

d. Scoring the Transition Course

(1) Scoring the Transition Course shall be done by counting the number of hits within the silhouette target to establish a satisfactory or unsatisfactory rating. An unsatisfactory rating merely indicates a need for additional training and development of basic skills.

(2) Rating with the 6-shot revolver:

Possible Score	-----	48
Satisfactory	-----	32+
Unsatisfactory	-----	31-

(3) Rating with the 5-shot revolver or semi-automatic pistol:

Possible Score	-----	40
Satisfactory	-----	27+
Unsatisfactory	-----	26-

6. Shotguns

a. Safety Rules

(1) When loading a shotgun, keep the weapon vertical to the ground, muzzle up.

(2) The safe condition of a shotgun is unloaded, action open, and safety on. When carrying the weapon on the range, when benching it, or receiving it from or handing it to another person, make certain it is in this condition.

(3) Never put a finger through the trigger guard to set or release safety.

(4) Never snap the trigger to release the action. Use the action release.

(5) After unloading a shotgun, visually examine the chamber and the magazine to make certain the weapon is unloaded.

(6) When transporting a shotgun in a vehicle, it is recommended that it be unloaded. When it becomes necessary to transport it in a loaded condition, a shell should not be chambered, but rather have four rounds in the magazine and the safety on.

(7) A shotgun will be brought to a firing position (i.e., leveled at the suspect or target) and the safety taken

off in preparing to fire. At all other times, when the security force personnel are on foot, the shotgun will be carried in a vertical or port arms position with safety on.

b. Combat Shotgun Course With Alternate

(1) This course is designed to provide training in safety, loading, and firing the shotgun from the hip and shoulder positions. The course is shot on a twenty-five yard range with firing point at fifteen and twenty-five yards. Normally, only one shooter will shoot at a time. Two shooters may fire at the same time if separated by a minimum of twenty feet and two qualified instructors are present. Five bobber (Army E) targets spaced four feet apart, numbered left to right, one through five, will be utilized. In the event that use of five closely spaced targets is not permitted or possible, then the alternate course of fire shall be used. Both the regular and alternate course of fire consist of three phases with a total of twelve rounds and will be fired once by each individual authorized to fire quarterly. The load for all phases will normally be 00-buckshot. There is no time limit on any phase of the shotgun course. Safety, familiarity, and accuracy should be stressed.

(2) Special Regulations and Instructions for the Combat Shotgun Course With Alternative

(a) Combat loading of the 12 gauge, model 870 type shotgun. The shooter will have the requisite number of shotgun shells in the non-shooting side front pants pocket. The muzzle of the shotgun is kept pointing downrange towards the target (target acquisition) with the slide pulled back. While looking only at the target, the shooter takes a shell from his or her pants pocket and cups the shell in the non-shooting hand. A right handed shooter must bring the shell underneath the weapon and roll the shell into the open chamber. He or she then moves the slide forward chambering the shell and enabling the weapon to be fired immediately. A left-handed shooter merely drops the shell into the open chamber. Other shells are also loaded by feel while the shooter's eyes maintain a visual on the target. The shells are tipped at a slight (less than 45 degree) angle and pushed into the magazine with the non-shooting hand. The muzzle remains pointed downrange towards the target.

(b) Combat Unloading. To unload live shells the weapon is again pointed downrange towards the target area. The slide is slowly pulled to the rear where the shell drops into the open chamber but will not be ejected. The shooter then rotates the weapon 180 degrees so that the open chamber faces the ground and the live shell drops into the shooter's

16 SEP 1985

non-shooting hand. The slide is moved forward and this action is repeated until all shells have been removed.

(c) Safe Weapon. The slide is pulled to the rear and the chamber and magazine are visually and physically checked with the fingers. The weapon is then placed on safe and held at "port arms" with the fingers of one hand curled inside the chamber.

(3) Regular Course of Fire

(a) Phase 1. Five rounds, three standing and two kneeling, from 25-yards. The shooter takes up a position on the 25-yard line with the shotgun at port arms, action open, and safety on. Five rounds of ammunition are in the left-front pants pocket (right-front pocket if left-handed). On command of the range officer, the shooter combat loads three rounds (one in the chamber), then assumes a port arms position facing the targets with the action closed and the safety on. When the commence fire signal is given, the shooter will bring the shotgun to the shoulder position (strong-hand), remove the safety, and fire three rounds, one each at three targets, in the order pre-directed by the range officer. After firing the three rounds, on command, the shooter will combat load two rounds (one in the chamber) and assume a port arms position facing the target. On the commence fire signal, the shooter will assume the kneeling position, remove the safety, and fire the two remaining rounds, one each at pre-directed targets designated by the range officer. After firing the two rounds, the shooter will open the action, put the safety on, hold the shotgun at port arms, and move forward on command to check the target. The shooter then returns to the 15 yard line for Phase 2.

(b) Phase 2. Five rounds, four from the hip and one from the kneeling strong shoulder position at 15 yards. On command of the range officer, the shooter combat loads three rounds (one in the chamber), then assumes a port arms position facing the targets with the action closed and the safety on. When the commence fire signal is given, the shooter assumes the hip position, removes the safety and fires three rounds, one each at three targets, in the order predirected by the range officer. After firing the three rounds, the action is opened, safety put on, and the shotgun held at port arms. On command, the shooter combat loads two rounds (one in the chamber) and assumes a port arms position facing the target. On the commence fire signal, the shooter assumes the hip position, removes the safety and fires one round. The shooter then assumes the kneeling position and fires the remaining round from the shoulder position (strong-hand). Both rounds are fired at pre-directed targets designated by the range officer. The

shooter then stands, opens the action, puts the safety on and holds the shotgun at port arms. On command, the shooter moves forward and checks the targets.

(c) Phase 3. Two rounds, fired from the shoulder position, weak-hand, at 15 yards. On command of the range officer, the shooter combat loads two rounds (one in the chamber), closes the action, releases the safety, and assumes proper port arms position for weak-hand position. When the commence fire signal is given, the shooter brings the shotgun to the weak-hand shoulder, and fires two rounds at two targets in the order pre-directed by the range officer. The action is then opened, the safety put on and the strong-hand port arms position assumed. On command, the target is checked after the shotgun is benched.

(4) Alternate Course of Fire

(a) The following course will be fired when range facilities do not allow for firing the basic shotgun course. This course consists of three phases, a total of twelve rounds; five rounds from 25 yards and seven rounds from 15 yards. The course will be fired by each individual and the ammunition and loading order for each phase will be the same as for the basic shotgun course.

(b) Phase 1. Five rounds, three standing and two kneeling from 25 yards. The shooter takes up a position on the 25 yard line with the shotgun at port arms, action open, and safety on. The shooter has five rounds of ammunition in the left-front pocket (right-front pocket if left-handed). On command of the range officer, the shooter combat loads three rounds (one in the chamber) and assumes a port arms position facing the target with the action closed and safety on. When the commence fire signal is given, the shooter brings the shotgun to the strong-hand shoulder, removes the safety, and fires three rounds. After firing the three rounds, the action is opened, safety put on, and shotgun held at port arms position. On command, at the 25 yard line, two rounds (one in the chamber) are combat loaded. When the commence fire signal is given, the shooter assumes the kneeling position, removes the safety and fires both rounds. The action is opened, safety put on and, with the shotgun at port arms, the shooter moves forward on command and checks the target for hits.

(c) Phase 2. Five rounds, four from the hip position and one from the kneeling position at 15 yards. On command of the range officer, the shooter combat loads three rounds (one in the chamber) and assumes the port arms position facing the targets with the action closed and safety on. When the commence fire signal is given, the shooter assumes the hip

16 SEP 1985

non-shooting hand. The slide is moved forward and this action is repeated until all shells have been removed.

(c) Safe Weapon. The slide is pulled to the rear and the chamber and magazine are visually and physically checked with the fingers. The weapon is then placed on safe and held at "port arms" with the fingers of one hand curled inside the chamber.

(3) Regular Course of Fire

(a) Phase 1. Five rounds, three standing and two kneeling, from 25-yards. The shooter takes up a position on the 25-yard line with the shotgun at port arms, action open, and safety on. Five rounds of ammunition are in the left-front pants pocket (right-front pocket if left-handed). On command of the range officer, the shooter combat loads three rounds (one in the chamber), then assumes a port arms position facing the targets with the action closed and the safety on. When the commence fire signal is given, the shooter will bring the shotgun to the shoulder position (strong-hand), remove the safety, and fire three rounds, one each at three targets, in the order pre-directed by the range officer. After firing the three rounds, on command, the shooter will combat load two rounds (one in the chamber) and assume a port arms position facing the target. On the commence fire signal, the shooter will assume the kneeling position, remove the safety, and fire the two remaining rounds, one each at pre-directed targets designated by the range officer. After firing the two rounds, the shooter will open the action, put the safety on, hold the shotgun at port arms, and move forward on command to check the target. The shooter then returns to the 15 yard line for Phase 2.

(b) Phase 2. Five rounds, four from the hip and one from the kneeling strong shoulder position at 15 yards. On command of the range officer, the shooter combat loads three rounds (one in the chamber), then assumes a port arms position facing the targets with the action closed and the safety on. When the commence fire signal is given, the shooter assumes the hip position, removes the safety and fires three rounds, one each at three targets, in the order predirected by the range officer. After firing the three rounds, the action is opened, safety put on, and the shotgun held at port arms. On command, the shooter combat loads two rounds (one in the chamber) and assumes a port arms position facing the target. On the commence fire signal, the shooter assumes the hip position, removes the safety and fires one round. The shooter then assumes the kneeling position and fires the remaining round from the shoulder position (strong-hand). Both rounds are fired at pre-directed targets designated by the range officer. The

shooter then stands, opens the action, puts the safety on and holds the shotgun at port arms. On command, the shooter moves forward and checks the targets.

(c) Phase 3. Two rounds, fired from the shoulder position, weak-hand, at 15 yards. On command of the range officer, the shooter combat loads two rounds (one in the chamber), closes the action, releases the safety, and assumes proper port arms position for weak-hand position. When the commence fire signal is given, the shooter brings the shotgun to the weak-hand shoulder, and fires two rounds at two targets in the order pre-directed by the range officer. The action is then opened, the safety put on and the strong-hand port arms position assumed. On command, the target is checked after the shotgun is benched.

(4) Alternate Course of Fire

(a) The following course will be fired when range facilities do not allow for firing the basic shotgun course. This course consists of three phases, a total of twelve rounds; five rounds from 25 yards and seven rounds from 15 yards. The course will be fired by each individual and the ammunition and loading order for each phase will be the same as for the basic shotgun course.

(b) Phase 1. Five rounds, three standing and two kneeling from 25 yards. The shooter takes up a position on the 25 yard line with the shotgun at port arms, action open, and safety on. The shooter has five rounds of ammunition in the left-front pocket (right-front pocket if left-handed). On command of the range officer, the shooter combat loads three rounds (one in the chamber) and assumes a port arms position facing the target with the action closed and safety on. When the commence fire signal is given, the shooter brings the shotgun to the strong-hand shoulder, removes the safety, and fires three rounds. After firing the three rounds, the action is opened, safety put on, and shotgun held at port arms position. On command, at the 25 yard line, two rounds (one in the chamber) are combat loaded. When the commence fire signal is given, the shooter assumes the kneeling position, removes the safety and fires both rounds. The action is opened, safety put on and, with the shotgun at port arms, the shooter moves forward on command and checks the target for hits.

(c) Phase 2. Five rounds, four from the hip position and one from the kneeling position at 15 yards. On command of the range officer, the shooter combat loads three rounds (one in the chamber) and assumes the port arms position facing the targets with the action closed and safety on. When the commence fire signal is given, the shooter assumes the hip

16 SEP 1985

position, removes the safety and fires three rounds. After firing the three rounds, the action is opened, safety put on and the shotgun is held at port arms. On command, at the 15 yard line, the shooter combat loads two rounds (one in the chamber) and assumes a port arms position facing the target with the action closed and safety on. When the commence fire signal is given, the shooter assumes the hip position, removes the safety, fires one round, then assumes the kneeling position and fires the remaining round. The shooter makes the shotgun safe (action open, safety on), holds the weapon at port arms, and on command, moves forward and checks the target.

(d) Phase 3. Two rounds fired from the shoulder position, weak-hand, at 15 yards. On command of the range officer, the shooter combat loads two rounds (one in the chamber), closes the action, releases safety, and assumes proper port arms position for weak-hand. When the commence fire signal is given, the shooter brings the shotgun to the weak-hand shoulder and fires two rounds. The shooter then opens the action, puts safety on, and assumes the port arms position. On command, the shooter moves forward and checks the target. Note: On ranges where hip level shooting with the shotgun is prohibited, the shoulder position may be substituted.

(5) Qualification. There will be no numerical qualification score for the shotgun. It will be the responsibility of the designated range officers to observe each individual during shotgun training sessions and to certify that the individual can safely handle and fire the shotgun with some degree of accuracy.

16 SEP 1985

position, removes the safety and fires three rounds. After firing the three rounds, the action is opened, safety put on and the shotgun is held at port arms. On command, at the 15 yard line, the shooter combat loads two rounds (one in the chamber) and assumes a port arms position facing the target with the action closed and safety on. When the commence fire signal is given, the shooter assumes the hip position, removes the safety, fires one round, then assumes the kneeling position and fires the remaining round. The shooter makes the shotgun safe (action open, safety on), holds the weapon at port arms, and on command, moves forward and checks the target.

(d) Phase 3. Two rounds fired from the shoulder position, weak-hand, at 15 yards. On command of the range officer, the shooter combat loads two rounds (one in the chamber), closes the action, releases safety, and assumes proper port arms position for weak-hand. When the commence fire signal is given, the shooter brings the shotgun to the weak-hand shoulder and fires two rounds. The shooter then opens the action, puts safety on, and assumes the port arms position. On command, the shooter moves forward and checks the target. Note: On ranges where hip level shooting with the shotgun is prohibited, the shoulder position may be substituted.

(5) Qualification. There will be no numerical qualification score for the shotgun. It will be the responsibility of the designated range officers to observe each individual during shotgun training sessions and to certify that the individual can safely handle and fire the shotgun with some degree of accuracy.

OPNAVINST 5530.14A
16 SEP 1985

UCMJ and JAG Manual
4th, 5th and 14th
Amendments
NAVEDTRA 10242
MCM 1950

JAG Manual
NAVEDTRA 10242
OPNAVINST 5580.1
MCM 1950
4th, 5th, 6th and
14th Amendments

JAG Manual
MCM 1950
NAVEDTRA 10242

OPNAVINST 5580.1
NAVEDTRA 10242
MCM 1950
JAG Manual
UCMJ

OPNAVINST 5580.1
NAVEDTRA 10242
MCM 1950

The trainee is introduced to the Military Rules of Evidence and applicable civilian rules, the kinds of evidence, the admissibility of evidence, the methods of distinguishing relevance from competency and materiality. The trainee discusses illegally obtained evidence, admissions, and confessions.

The trainee is introduced to and informed of the basic principles which constitute a lawful search and/or seizure. The trainee should also receive a basic understanding of the laws and judicial interpretations that make them lawful, stressing probable cause. The trainee should be familiar with search warrants and the procedural steps for securing same.

The trainee is presented the fundamentals of substantive criminal law relative to the definitions and classifications of crimes in general.

The trainee is presented the use of Article 31, UCMJ and the 5th, 6th, and 14th Amendments to the U.S. Constitution as they pertain to obtaining statements or admissions from the accused, witnesses, and suspects. The trainee reviews the right of the individual to due process of law, to have counsel, the privilege against self-incrimination, the personal nature of the self-incrimination waiver, the warning requirements contained in the various Federal Statutes.

The trainee identifies the elements of a legal arrest/apprehension and distinguishes situations involving mere suspicion, and probable cause. The trainee should

les of Evidence

earch and Seizure

ubstantive Criminal Law

elf-Incrimination,
Admissions and
Confessions

pprehension and Arrest
Stop and Frisk

also be able to identify the essential criteria for making a stop and frisk.

Detention and Confinement

The trainee is given a brief overview of the administration, management, and operation of a Navy Brig and detention cell as well as the current philosophy and organization of the Navy's Corrections Program.

SECNAVINST 1640.10
OPNAVINST 5580.1
SECNAVINST 1640.9A
BUPERSINST 1640.17

Federal Magistrate System

The trainee is introduced to the military and federal magistrate system including the Assimilative Crimes Act as it applies to application of state vehicle laws on naval installations having exclusive or concurrent federal legislative jurisdiction.

SECNAVINST 5822.1
NAVEDTRA 10242

Status of Forces Agreement

As applicable, the trainee should discuss the implication and meaning of sovereignty in international law and the role and purposes of international agreements pertaining to jurisdiction with emphasis placed on the Status of Forces Agreement.

DOD Directive 5525.1
(NOTAL)

TRAFFIC LAWS AND ENFORCEMENT

Military Traffic Law and Enforcement

The trainee will receive the policies, responsibilities, and procedures for motor vehicle traffic supervision, including the traffic federal magistrate system and the mechanics of military and federal citation issuance (DD Forms 1407 and 1805). The trainee should discuss the safe and efficient movement of vehicles, material, and personnel to, from, and onboard the command.

OPNAVINST 11200.5B
OPNAVINST 5100.12B
SECNAVINST 5822.1

16 SEP 1985

JAG Manual
NAVEDTRA 10242
OPNAVINST 11200.5B

The trainee should be provided with a basic knowledge of how to investigate a motor vehicle accident and a flexible plan of action to deal with all phases involving accidents. The trainee is instructed on how to properly prepare and complete accident reports and related documents. A brief overview of JAG investigations of government vehicle accidents should be presented.

OPNAVINST 5580.1
NAVEDTRA 10242
Assimilative
Crime Act
JAG Manual and USMJ

The trainee must be impressed with the seriousness of the drunk driving problem and its effect on accident and death rates. The trainee is instructed in the techniques for detecting, apprehending, and testing persons suspected of driving under the influence of intoxication. The trainee should be familiar with field sobriety testing and the preparation of the DD Form 1920 (Alcoholic Influence Report) in examining, interpreting, and recording results of such tests.

OPNAVINST 5580.1
Army Field Manual
19-10

The trainee discusses the basic principles of military traffic control as well as the methods and techniques of traffic control. The trainee should discuss various traffic situation, the establishment of traffic and tactical posts, controlling traffic flow, hand and arm signals, and directing traffic during the hours of darkness.

OPNAVINST 5580.1
OPNAVINST 11200.5
Uniform Vehicle Code
Assimilative Crime Act

The trainee is presented local command parking rules, regulations, and laws with the aim of the most efficient use of existing on- and off-street parking facilities. The trainee should learn when the temporary impoundment of vehicles is authorized and the procedures for effecting same.

ATROL PROCEDURES

Radio Communications
"10" Code

The trainee is presented with the procedures for communications to include types of calls, phonetic alphabet, 24-hour time, the "10" code, the correct construction and delivery of messages, as well as receiving and recording messages. The trainee should also be familiarized with the command radio and telecommunications systems applicable to law enforcement with emphasis placed upon messages and message forms.

OPNAVINST 5580.1
Chapter 10

Traine and Specialized
Building and Repository
escorts

The trainee is presented the primary purposes of patrols which are to protect life and property, deter crime, supervise road traffic laws and regulations, maintain good order and discipline, furnish information and direction, and perform escort and building checks. Types of patrols including vehicle, bicycle, foot, or reserve/special, and methods of patrol such as varying routes and times of patrols should be presented.

OPNAVINST 5580.1
NAVEDTRA 10242

Vehicle Stops
Search of Vehicles

The trainee will develop an ability to make safe, effective vehicle stops and control situations that escalate after the stop. Search of vehicles should be discussed in depth, supported by legal decisions as to when and where they are constitutionally legal.

OPNAVINST 5580.1
NAVEDTRA 10242
Applicable state and
Federal laws and
statutes.

Trains in Progress

The trainee is instructed with regard to the proper response to a crime in progress emphasizing safe, effective driving, approach, arrival, duties and responsibilities at the scene, search of the area, and inherent dangers such as ambush, attacks, terrorists, etc.

OPNAVINST 5580.1
NAVEDTRA 10242

Physical Security
Safeguards

10 SEP 1953
OPNAVINST 5530.14
Local Directives
and guidance.
OPNAVINST 5530.13

The trainee will be completely indoctrinated and familiar with the command physical security safeguard requirements and policies including perimeter gates and fences; protective lighting; intrusion detection systems, their locations, purpose and required response times; key and lock control systems, etc.

5. UNUSUAL INCIDENTS

Terrorism

OPNAVINST 5580.1
OPNAVINST 5530.15
OPNAVINST 3850.4A
Applicable local
guidance and
directives

The trainee is provided with an orientation to terrorism emphasizing any group or groups known or suspected to be operational in the area. The trainee should become familiar with the types of violence, motivational factors, targets, cell structure of the group(s), etc. Responses to terrorists actions and preventive measures should be discussed.

Bomb Threats, Wrongful
Destruction and Sabotage

OPNAVINST 5580.1
OPNAVINST 5530.14
NAVEDTRA 10242
Local directives
and guidance.

The trainee should be able to develop a plan of action to be taken upon receipt of, during, and after a bomb threat including when or where not to evacuate. The trainee should discuss the differences between destruction and sabotage, stressing intent and the military and federal criminal laws applicable.

6. PROFESSIONAL SKILLS

Driver Training

Within available means, all-three components, i.e., basic knowledge for emergency vehicle operators, specialized police service, and in-vehicle skill development, of the U.S. Department of Transportation, National Highways Traffic Safety Administration's Emergency Vehicle Operator Course (DOT EVOC) may be presented

to the trainee as set forth in paragraph 0910 of this instruction. Practical exercises should be presented during this instruction for vehicle stops, transporting prisoners, and removal of reluctant prisoners. Care and maintenance of emergency vehicles should also be discussed.

b. Weapons Proficiency
Training

The trainee is familiarized with the nomenclature and rules pertaining to the safe handling and operation of weapons utilized by the security department. Care and maintenance of weapons should be stressed and proper techniques for same presented. The trainee should be familiarized with range safety procedures, commands, and utilization procedures and the requirements for strict compliance. The trainee should be expected to develop a high degree of proficiency in their handling of issued weapons, including shotguns, if utilized, through expert instruction and the practical courses of fire as set forth in this instruction.

OPNAVINST 5580.1
SECNAVINST 5500.32
Appendix XIII Tab A
of this instruction.

c. Use of Force
Minimum
Deadly

The trainee is presented the use and types of force to be employed in a variety of situations, stressing the requirement for use of minimum force. The trainee should discuss legal, moral, and ethical considerations involved in the use of deadly force and develop sound judgement to formulating decisions regarding the use of force.

OPNAVINST 5580.1
SECNAVINST 5500.29A
Chapter 9, of
this instruction.

d. Defensive Tactics

The trainee observes a demonstration, then achieves proficiency through practical exercises in the basic principles of unarmed self-defense

OPNAVINST 5580.1
NAVEDTRA 10242
FBI "Defensive
Tactics, A Manual

The trainee will learn the baton come-alongs and defensive uses to avoid losing control. Apprehension, search, and restraint techniques should also be demonstrated and practiced during this session, stressing handcuffing techniques.

e. Physical Training

Prior to the commencement of any block of training in which physical exertion or exercise is required, the trainee must have been rendered physically fit for this type of exertion by completion of the physical training program

OPNAVINST 5580.1
 OPNAVINST 6110.1
 Presidents Council
 for Physical Fitness
 FBI's "Physical
 Fitness for Law
 Enforcement
 Officers"

VINST 5530.14A
SEP 1985

LAW ENFORCEMENT/PHYSICAL SECURITY
TRAINING COURSE - PHASE TWO

SUGGESTED
REFERENCE MATERIAL

SCOPE

SUBJECT

ADMINISTRATIVE SUBJECTS

Recording, Handling and
Disposition of Property
Missing, Lost, Stolen,
or Recovered (MLSR)

The trainee is taught the procedures for the recording, handling, and disposition of the various types of property coming into the custody of the security department, emphasizing special procedures for evidence. The trainee is taught the policy and procedures for reporting missing, lost, stolen, or recovered (MLSR) government property.

SECNAVINST 5500.4D
OPNAVINST 5580.1

Information Security

The trainee will be introduced to the command Information Security Program and their responsibility for compliance with all of the legally established directives regarding the protection of classified information and material.

OPNAVINST 5510.1G
Local Directives
and guidance.

Absentees and Deserters

The trainee is introduced to the policy and procedures for the handling of absentees and deserters coming into their custody. The trainee should be made aware of the Navy's Deserter Apprehension Program, in general, and the Absentee Collection Units, in particular.

SECNAVINST 1620.7

Public Relations

The trainee is introduced to the elements essential to building and maintaining a positive and constructive climate for security force personnel/citizen interaction.

Local directives
and guidance.

2. LEGAL SUBJECTS

Juvenile Offenses

The trainee is presented the authority of law enforcement personnel with regard to the enforcement of juvenile matters on federal, state, and military jurisdictions and overseas installations. The trainee should be familiarized with the Juvenile Justice and Delinquency Prevention Act, Public Law 93-415 of 1974

OPNAVINST 5580.1
NAVEDTRA 10242

Judicial Proceedings Testimony and Demeanor

The trainee is presented the jurisdictional limitations of non-judicial punishment and duties of the Master-at-Arms and military and civilian law enforcement personnel in conjunction with Captain's Mast, courts of inquiry, civilian courts, and courts martial. The trainee should be familiar with courtroom procedures, demeanor, attitudes, and methods of addressing questioner.

SECNAVINST 1640.10
NAVEDTRA 10242
JAG Manual and UCMJ

3 TRAFFIC LAWS AND ENFORCEMENT

Selective Enforcement

The trainee is presented the planned distribution of security force personnel and equipment, including radar, where and when needed to deter violations which contribute to increased accidents or congestion. This block can also be made applicable to crime prevention and enforcement.

OPNAVINST 5580.1
NAVEDTRA 10242
Army Field Manual
19-10

Crime Prevention

The trainee is presented those actions which law enforcement personnel can take to prevent crime as well as how they can involve the community-at-large (military and civilian) through education and participation. The trainee should be introduced to and learn how to conduct the various forms of crime prevention surveys, i.e., internal, external, spot, etc.

OPNAVINST 5580.1

2-4. CRIMINAL INVESTIGATIONS

a. Jurisdiction and
Responsibilities
Felonies

The trainee is presented the duties and those responsible for the investigation of crimes and security breaches on board the command, what constitutes a major versus a minor crime, action to be taken when those responsible are not available, and other related matters. The individual roles of NIS, command investigators, the Master-at-Arms Force, Shore Patrol, FBI, and other law enforcement agencies should be discussed.

OPNAVINST 5580.1
SECNAVINST 5520.3
SECNAVINST 5820.1
Local directives
and guidance.

b. Crime Scenes
Identification,
Preservation,
and Collection of
Evidence, Notes,
Sketches and Photography

Emphasis is placed upon the importance of the preservation of the crime scene to the trainee. The trainee should be introduced to the identification of physical evidence in a crime scene setting, if possible, the techniques of searching for evidence, the necessity for a sketch and how to draw one, stressing essential elements; notes and records to be kept and, crime scene photography with instruction in the operation of the camera(s) in use at the security department.

OPNAVINST 5580.1
NAVEDTRA 10242
Local directives
and guidance

c. Identification of Victims,
Witnesses, and Suspects
Showups
Lineups

The trainee is acquainted with the proper methods of identifying victims, witnesses, missing persons, suspects, and deceased persons. Stress the importance of accurate identification and relate how this information can aid in the successful conclusion of an investigation. The trainee discusses the use of line-ups and street showups as a method of identification with emphasis on the mechanics of properly conducting them, time constraints involved, and other mitigating factors.

OPNAVINST 5580.1
NAVEDTRA 10242
Local directives
and guidance

Interviews and
Interrogations
Notetaking
Statements

The trainee should be instructed with liberal use of practical exercises in the proper techniques of approach, along with the types of questions to ask when conducting interviews and interrogations. The trainee will be taught to prepare written statements and interview summaries.

OPNAVINST 5580.1
NAVEDTRA 10242
Local directives
and guidance

Managing Informants

The trainee is shown the importance of sources and informants in the successful conduct of investigations. The trainee is introduced to some of the techniques to recruit informants. Overall, the trainee will learn to identify requirements for developing and safeguarding informants.

OPNAVINST 5580.1
Local directives
and guidance

Crimes Against Persons

The trainee is presented the elements, proof required, procedures, and objectives for the investigation of such crimes against persons as homicide, sex offenses, robbery, assault, etc. Each trainee should know how to conduct a thorough preliminary investigation until the arrival of the agent or investigator with jurisdiction and responsibility.

OPNAVINST 5580.1
NAVEDTRA 10242
Local directives
and guidance

Crimes Against Property

The trainee is presented the proof required, procedures, for the investigation of such crimes against property as burglary, auto theft, arson, check fraud, etc. MLSR requirements should be reviewed again as well as the requirements for entry of information into NCIC or other federal military computer systems.

Elements,
Objectives
Crimes
Arson, etc.
Theft, etc.
Property
Theft, or

OPNAVINST 5580.1
NAVEDTRA 10242
Local directives
and guidance

16 SEP 1963

Interviews and
Interrogations
Notetaking
Statements

The trainee should be instructed with liberal use of practical exercises in the proper techniques of approach, along with the types of questions to ask when conducting interviews and interrogations. The trainee will be taught to prepare written statements and interview summaries.

Managing Informants

The trainee is shown the importance of sources and informants in the successful conduct of investigations. The trainee is introduced to some of the techniques to recruit informants. Overall, the trainee will learn to identify requirements for developing and safeguarding informants.

Crimes Against Persons

The trainee is presented the elements, proof required, procedures, and objectives for the investigation of such crimes against persons as homicide, sex offenses, robbery, assault, etc. Each trainee should know how to conduct a thorough preliminary investigation until the arrival of the agent or investigator with jurisdiction and responsibility.

Crimes Against Property

The trainee is presented the elements, proof required, procedures, and objectives for the investigation of such crimes against property as burglary, larceny, auto theft, arson, check and fraud, etc. MLSR requirements should be reviewed again as well as the requirements and criteria for entry of items of property into NCIC or other federal, state, or military computer systems.

OPNAVINST 5580.1
NAVEDTRA 10242
Local directives
and guidance

OPNAVINST 5580.1
Local directives
and guidance

OPNAVINST 5580.1
NAVEDTRA 10242
Local directives
and guidance

OPNAVINST 5580.1
NAVEDTRA 10242
Local directives
and guidance

2-4. CRIMINAL INVESTIGATIONS

- a. Jurisdiction and
Responsibilities
Felonies

The trainee is presented the duties and those responsible for the investigation of crimes and security breaches on board the command, what constitutes a major versus a minor crime, action to be taken when those responsible are not available, and other related matters. The individual roles of NIS, command investigators, the Master-at-Arms Force, Shore Patrol, FBI, and other law enforcement agencies should be discussed.

OPNAVINST 5580.1
SECNAVINST 5520.3
SECNAVINST 5820.1
Local directives
and guidance.

- b. Crime Scenes
Identification,
Preservation,
and Collection of
Evidence, Notes,
Sketches and Photography

Emphasis is placed upon the importance of the preservation of the crime scene to the trainee. The trainee should be introduced to the identification of physical evidence in a crime scene setting, if possible, techniques of searching for evidence, the necessity for a sketch and how to draw one, stressing essential elements; notes and records to be kept and, crime scene photography with instruction in the operation of the camera(s) in use at the security department.

OPNAVINST 5580.1
NAVEDTRA 10242
Local directives
and guidance

- c. Identification of Victims,
Witnesses, and Suspects
Showups
Lineups

The trainee is acquainted with the proper methods of identifying victims, witnesses, missing persons, suspects, and deceased persons. Stress the importance of accurate identification and relate how this information can aid in the successful conclusion of an investigation. The trainee discusses the use of line-ups and street showups as a method of identification with emphasis on the mechanics of properly conducting them, time constraints involved, and other mitigating factors.

OPNAVINST 5580.1
NAVEDTRA 10242
Local directives
and guidance

Civil Disturbances,
Crowd/Mob
Psychology and Control

The trainee should be made aware of the responsibilities for the protection of government property and functions as well as the legal restrictions involved with that protection. Use of minimum force policies and riot control agents should be discussed along with the basic formations, weapons, moves, and commands utilized for mob and crowd control.

OPNAVINST 5580.1
NAVEDTRA 10242
Applicable local
directives and
guidance.

Hostage Situations and
Barricaded Suspect(s)
Scene Security,
Notifications

The trainee is presented the various actions to be taken and notifications to be made upon arrival at the scene of a hostage situation or barricaded suspect. The basic responses available to law enforcement personnel in barricaded suspect/hostage situations and the various weapons, tactics, and actions to be taken for each different response should be presented.

OPNAVINST 5580.1
NAVEDTRA 10242
Applicable local
directives and
guidance.
OPNAVINST 5530.15

Animal Complaints

The trainee is presented those actions to be taken and/or notifications made in response to an animal complaint; particular emphasis being placed on procedures in the event of an animal bite and/or rabid animal. The trainee should be familiarized with those organizations, military and civilian, who will assist with, and respond to, animal incidents and remove same, if necessary.

Local directives
and guidance.
State and local
shelters and SPCA.

Services
to Persons,
Children and
the Persons

The trainee should receive the definitions, report requirements, and classifications of missing persons with emphasis on children. The trainee should be able to determine the difference between a critical and non-critical missing person

Local directives
and guidance.
Local Children's
shelters and
other agencies.

OPNAVINST 5530.14A
16 SEP 1985

h. Drugs of Abuse
Identification,
Prevention and
Control

The trainee should develop an ability to identify current drugs of abuse, utilizing not only generic names, but also street parlance. Additionally, a controlled burn should be conducted to familiarize the trainee with the odor of marijuana, and a record of this made in their service and/or training record. The trainee should discuss the particular drug problems of your command, as well as the Navy's effort to combat the overall problem.

OPNAVINST 5580.1
OPNAVINST 5350.4
NAVEDTRA 10242
AMA's "Drug Abuse:
A Guide for the
Primary Care
Physician"

i. Vice Investigations,
Armed Forces
Disciplinary Boards

Discussion should be held with the trainee on the Armed Forces Disciplinary Control Boards (AFDCB's) and their mission, function, organization, limitations, and authority. The on- or off-installation drug, alcohol, or vice conditions negatively impacting upon the mission should also be discussed.

OPNAVINST 1620.1A
Local directives
and guidance.

2-5. UNUSUAL INCIDENTS.

a. Disaster and Emergency
Planning

The trainee is presented the various activity disaster and emergency bills with emphasis on their roles in the movement of essential traffic to, from, and within the stricken area; prevention of further loss of life and protection of property; care of living casualties; and recovery, removal, identification, and disposition of the fatally injured. The trainee should also be thoroughly familiar with those notifications and initial actions required by them in the event of any such emergency or disaster.

OPNAVINST 5580.1
Applicable local
directives and
guidance.

16 SEP 1983

Local directives
and guidance.

security department and when their use is justified, e.g., riots, uncontrollable persons, etc. The trainee should not only learn how to operate these devices but also know how to render first aid after their use.

Breath Testing and Radar Certification

Through lecture and practical exercise the trainee will learn the proper procedures for setting up, calibrating, testing, and operating radar and the breath testing equipment utilized by the security department. Upon successful completion of the lectures, written examinations, and practical applications should be given to enable the trainee to obtain certifications for these devices from the state or jurisdiction wherein they are authorized.

Fingerprints Rolled and Latent

The trainee is presented with the practical aspects relating to the use and recognition of fingerprint patterns the development of skills in taking rolled impressions, and the processing of latent prints for identification and use as evidence. Each student must demonstrate skill in practical exercises developing latent and rolled prints.

FBI's "The Science of
Fingerprints:
Classification and
Uses".

FBI's "Techniques for
Taking Good Finger-
prints"

Agency Medicine/Trauma Management

The trainee is shown how to administer proper medical care to victims of disasters, illness, accidents, and other trauma events when confronted with situation that require emergency medical management techniques. Trainee should satisfactorily complete either the Navy's Standard First Aid Training Course or the American Red Cross Multi-media Standard

and those actions and notifications necessary for each category. Procedures for handling found children and senile persons should be outlined in detail.

ly Intervention
use Abuse
ld Abuse
estic Conflict

The trainee is introduced to and discusses the dangers inherent in crisis intervention within the domestic setting. The need for sensitive but thorough investigation in areas such as child abuse, incest, spouse abuse, and other offenses directed against children and the family should be discussed. Also presented should be those military and civilian agencies and advocate groups available to assist with child and/or family crisis situations. Effective crisis intervention techniques should be developed by the trainee by not only lecture but also practical exercises involving hypothetical situations.

OPNAVINST 5580.1
Local directives
and guidance
NAVEDTRA 10242
Local charitable
agencies and
and church groups.

gnizing and Handling
rmal Behavior
coholism
ug Abuse
ntal Disorders

The trainee is presented three areas of abnormal behavior, i.e., mental illness, mental retardation, and psychopathic personality. The trainee should be presented with the specific symptoms for the recognition of behavior in each of these areas and the generally recommended methods for dealing with each. The trainee should discuss the symptoms of drug and alcohol abuse, emergency and medical treatment, and handling these individuals in possible violent situations.

National Mental Health
Association "How to
Recognize and Handle
Abnormal People: A
A Guide for Police
Officers"

PROFESSIONAL SKILLS

ical Agents

The trainee will become acquainted with the various chemical agents used by the

OPNAVINST 5580.1
NAVEDTRA 10242

Physical Training

First Aid Course. The trainee must satisfactorily complete the American Heart Association CPR course and receive a certification.

The trainee should continue physical training through Phase Two of initial training.